201530344

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201530344 A

(43)公開日： 中華民國 104 (2015) 年 08 月 01 日

(21)申請案號：103102096 (22)申請日： 中華民國 103 (2014) 年 01 月 21 日

(51)Int. Cl.： *G06F21/55 (2013.01)* *G06F21/57 (2013.01)*

(71)申請人：周宏建 (中華民國) (TW)

臺中市南屯區永春東路 1000 之 19 號 12 樓

(72)發明人：周宏建 (TW)

(74)代理人：高玉駿；楊祺雄

申請實體審查：有 申請專利範圍項數：20 項 圖式數：3 共 26 頁

(54)名稱

應用程式存取保護方法及應用程式存取保護裝置

(57)摘要

一種應用程式存取保護方法，包含以下步驟：(A)一具有一第一認證資料及一第一控制規範之應用程式存取保護裝置判定執行於一作業系統中之一待比對應用程式是否具有該第一認證資料及第一控制規範；及(B)在該步驟(A)之判定結果為否之情況下，表示該待比對應用程式為一無法被授權之非法應用程式，且該應用程式存取保護裝置不允許該非法應用程式控制一受控裝置。

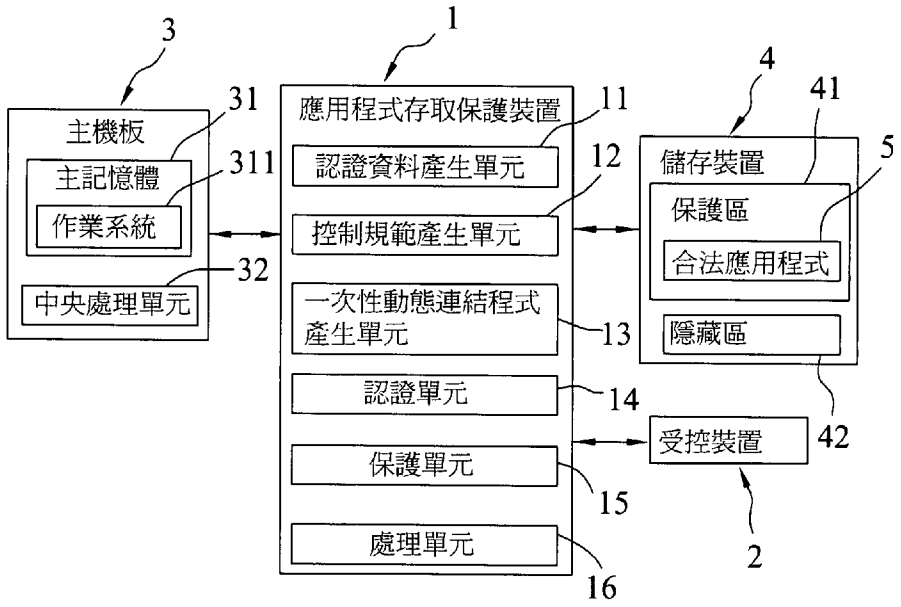

圖1

1・・・應用程式存取保護裝置

11・・・認證資料產生單元

12・・・控制規範產生單元

13・・・一次性動態連結程式產生單元

14・・・認證單元

15・・・保護單元

16・・・處理單元

2・・・受控裝置

3・・・主機板

31・・・主記憶體

311・・・作業系統

32・・・中央處理單元

4・・・儲存裝置

41・・・保護區

42・・・隱藏區

5・・・合法應用程式

201530344

發明摘要

※ 申請案號：103102096

※ 申請日：103.1.21　　※IPC 分類：G06F 21/55 (2013.01)　G06F 21/57 (2013.01)

【發明名稱】 應用程式存取保護方法及應用程式存取保護裝置

【中文】

一種應用程式存取保護方法，包含以下步驟：(A)一具有一第一認證資料及一第一控制規範之應用程式存取保護裝置判定執行於一作業系統中之一待比對應用程式是否具有該第一認證資料及第一控制規範；及(B)在該步驟(A)之判定結果爲否之情況下，表示該待比對應用程式爲一無法被授權之非法應用程式，且該應用程式存取保護裝置不允許該非法應用程式控制一受控裝置。

【英文】

【代表圖】

【本案指定代表圖】：圖（ 1 ）。

【本代表圖之元件符號簡單說明】：

1……應用程式存取保護裝置

11……認證資料產生單元

12……控制規範產生單元

13……一次性動態連結程式產生單元

14……認證單元

15……保護單元

16……處理單元

2……受控裝置

3……主機板

31……主記憶體

311……作業系統

32……中央處理單元

4……儲存裝置

41……保護區

42……隱藏區

5……合法應用程式

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

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】 應用程式存取保護方法及應用程式存取保護裝置

【技術領域】

【0001】 本發明是有關於一種應用程式存取保護方法，特別是指一種防止一非法應用程式控制一受控裝置的應用程式存取保護方法及應用程式存取保護裝置。

【先前技術】

【0002】 由於現今資訊科技的發達與普及，各種便利的應用程式也應勢而生。不論是應用程式使用者或是應用程式服務的提供者都在意所提供的功能服務是否有足夠的安全性考量，若應用程式被駭客植入惡意程式，而在使用者執行的過程中，盜取其隱私資料、破壞使用者的文件或操作畫面等，將會造成使用者的個人重要資料外洩或損毀，導致無法彌補的重大損失。

【0003】 因此，如何有效防止因應用程式被仿冒、竄改或植入惡意程式，而造成個人重要資料被竊取或損毀，遂成爲亟待解決之課題。

【發明內容】

【0004】 因此，本發明之目的，即在提供一種有效防止非法應用程式控制受控裝置的應用程式存取保護方法。

【0005】 於是本發明應用程式存取保護方法，包含以下

步驟：(A)一具有一第一認證資料及一第一控制規範之應用程式存取保護裝置判定執行於一作業系統中之一待比對應用程式是否具有該第一認證資料及第一控制規範；及(B)在該步驟(A)之判定結果爲否之情況下，表示該待比對應用程式爲一無法被授權之非法應用程式，且該應用程式存取保護裝置不允許該非法應用程式控制一受控裝置。

【0006】 本發明之另一目的，即在提供一種有效防止非法應用程式控制受控裝置的應用程式存取保護裝置。

【0007】 於是本發明應用程式存取保護裝置，適用於判定是否允許執行於一作業系統中的一待比對應用程式控制一受控裝置，該應用程式存取保護裝置包含一認證資料產生單元、一控制規範產生單元及一認證單元。該認證資料產生單元用以產生一第一認證資料。該控制規範產生單元用以產生一第一控制規範。該認證單元用以判定執行於該作業系統中之待比對應用程式是否具有該第一認證資料及第一控制規範，若判定結果爲否，表示該待比對應用程式爲一無法被授權之非法應用程式，且該認證單元不允許該非法應用程式控制該受控裝置。

【0008】 本發明之功效在於，藉由該應用程式存取保護裝置判定執行於該作業系統中之該待比對應用程式是否具有該第一認證資料及第一控制規範，以避免無該第一認證資料及第一控制規範的非法應用程式控制該受控裝置，進而避免電腦遭受電腦病毒感染。

【圖式簡單說明】

【0009】 本發明之其他的特徵及功效，將於參照圖式的實施方式中清楚地呈現，其中：

圖 1 是一系統方塊圖，說明本發明應用程式存取保護裝置之較佳實施例；

圖 2 是一流程圖，說明本發明應用程式存取保護方法之較佳實施例中的認證過程；及

圖 3 是一流程圖，說明本發明應用程式存取保護方法之較佳實施例中的再次認證過程。

【實施方式】

【0010】 參閱圖 1，本發明應用程式存取保護裝置 1 之較佳實施例，適用於判定是否允許執行於一作業系統 311 中的一待比對應用程式控制一受控裝置 2。該應用程式存取保護裝置 1 包含一認證資料產生單元 11、一控制規範產生單元 12、一次性動態連結程式產生單元 13、一認證單元 14、一保護單元 15 及一處理單元 16。值得一提的是，該應用程式存取保護裝置 1 是以韌體方式實現，其實施態樣可爲一晶片，可將該晶片安裝於個人電腦、筆記型電腦、平板電腦、智慧型手機或包含該儲存裝置與該受控裝置的計算系統等，當將該晶片安裝於該個人電腦時，該個人電腦即包含該應用程式存取保護裝置 1、一主機板 3、該受控裝置 2 及一儲存裝置 4。

【0011】 該主機板 3 包括一主記憶體 31 及一中央處理單元 32。

【0012】 該受控裝置 2 可包含安全元件（如，近場通訊

元件）、儲存元件（如，硬碟、快閃記憶體或其他任何形態的儲存元件）及週邊元件（如，鍵盤、滑鼠等）之至少一者。

【0013】該認證資料產生單元 11 用以產生一第一認證資料，其中該第一認證資料包含一個一次性認證演算法、一個一次性密鑰或一個一次性認證碼。

【0014】該控制規範產生單元 12 用以產生一第一控制規範，其中該第一控制規範包含一個一次性存取規範及一個一次性指令規範之至少一者。該一次性存取規範係爲一合法應用程式 5 傳送指令至該處理單元 16 的存取規範，例如，制定該合法應用程式 5 是否可以存取該受控裝置 2 之安全元件、儲存元件及週邊元件的規範、該合法應用程式 5 是否可以改變儲存於該儲存裝置 4 之一保護區 41 內的檔案的存取屬性的規範及該合法應用程式 5 傳送該指令至該處理單元 16 以存取該儲存裝置 4 之一隱藏區 42 的存取規範，其中該隱藏區 42 無法被該作業系統 311 辨識、讀取與寫入。該一次性指令規範係爲該處理單元 16 與該合法應用程式 5 對該指令的編碼規範，例如，定義該合法應用程式 5 與該處理單元 16 之間的指令編碼(0000 是讀取指令及 0001 是寫入指令等)。值得特別說明的是，配合不同的合法應用程式，該認證資料產生單元 11 及該控制規範產生單元 12 可產生不同的第一認證資料及第一控制規範。

【0015】該一次性動態連結程式產生單元 13 用以根據該第一認證資料及該第一控制規範產生一第一一次性動態連

結程式，其中該第一一次性動態連結程式爲可直接被該作業系統 311 執行的程式。值得特別說明的是，在本較佳實施例中，該一次性動態連結程式產生單元 13 會將該第一認證資料及該第一控制規範包含於該第一一次性動態連結程式再提供給該合法應用程式 5，該合法應用程式 5 再根據該第一一次性動態連結程式產生該第一認證資料及該第一控制規範，然而該第一認證資料及該第一控制規範亦可分別提供給該合法應用程式 5，而不將該第一認證資料及該第一控制規範結合成該第一一次性動態連結程式，並不以本發明說明書所揭示之方式爲限。

【0016】 由於該應用程式存取保護裝置 1 介於該受控裝置 2 與該運行於該主記憶體 31 的作業系統 311 之間，因此執行於該作業系統 311 中之待比對應用程式需完成與該應用程式存取保護裝置 1 之認證單元 14 的雙向認證，才能控制該受控裝置 2，以下將詳細說明該認證單元 14 之運作。

【0017】 該認證單元 14 用以判定執行於該作業系統 311 中之待比對應用程式是否具有該第一認證資料及第一控制規範。若判定結果爲否，表示該待比對應用程式爲一無法被授權之非法應用程式，且該認證單元 14 不允許該非法應用程式控制該受控裝置 2；若判定結果爲是，該認證單元 14 接收該待比對應用程式的第一認證資料以對該待比對應用程式進行認證，且該認證單元 14 傳送該認證資料產生單元 11 所產生的第一認證資料至該待比對應用程式，以供該待比對應用程式接收該第一認證資料以對該應用程式存取

保護裝置 1 進行認證。

【0018】 當該認證單元 14 與該待比對應用程式完成彼此間的雙向認證後，表示該待比對應用程式即爲該合法應用程式 5，該合法應用程式 5 將一符合該第一控制規範的指令以該合法應用程式 5 的第一認證資料加密後傳送至該處理單元 16，該認證單元 14 啓動該處理單元 16，使該處理單元 16 接收該加密後的指令且根據該第一認證資料解密該指令，繼而該處理單元 16 根據該解密後的指令控制該受控裝置 2，藉以使得該合法應用程式 5 可經由該處理單元 16 控制該受控裝置 2。也就是說，執行於該作業系統 311 中之合法應用程式 5 於完成雙向認證後亦無法直接控制該受控裝置 2，該合法應用程式 5 須透過該應用程式存取保護裝置 1 的該處理單元 16 才能控制該受控裝置 2。

【0019】 此外，由於該應用程式存取保護裝置 1 介於該儲存裝置 4 與該運行於該主記憶體 31 的作業系統 311 之間，因此該作業系統 311 在從該儲存裝置 4 之保護區 41 內讀取該合法應用程式 5 時，須經由該應用程式存取保護裝置 1 才能讀取該合法應用程式 5，且該應用程式存取保護裝置 1 之保護單元 15 會將該第一一次性動態連結程式提供給該合法應用程式 5，以下將詳細說明該保護單元 15 之運作。

【0020】 該保護單元 15 用以在該作業系統 311 從該儲存裝置 4 之保護區 41 內讀取該合法應用程式 5 及其對應的一預設一次性動態連結程式時，將該第一一次性動態連結程式傳送給執行於該作業系統 311 中的合法應用程式 5，以取

代該預設一次性動態連結程式，其中該作業系統 311 無法對該保護區 41 內的合法應用程式 5 進行刪除與寫入。在本較佳實施例中，該合法應用程式 5 及該預設一次性動態連結程式屬於兩個分開的檔案，該作業系統 311 可分別讀取該合法應用程式 5 及該第一一次性動態連結程式，亦即先讀取該合法應用程式 5，再讀取該取代該預設一次性動態連結程式的第一一次性動態連結程式。然而，在其他實施例中，該合法應用程式 5 及對應的預設一次性動態連結程式屬於同一個檔案，亦即，該合法應用程式 5 包含一應用子程式及該預設一次性動態連結程式，該作業系統 311 即無法分別讀取該合法應用程式 5 及該第一一次性動態連結程式，而須待該預設一次性動態連結程式已被該第一一次性動態連結程式取代後，再讀取該包含該應用子程式及該第一一次性動態連結程式的合法應用程式 5。

【0021】 當該認證單元 14 與該待比對應用程式須進行再次認證時，該認證資料產生單元 11 還用以產生一第二認證資料，該控制規範產生單元 12 還用以產生一第二控制規範，其中該第二認證資料包含另一個一次性認證演算法、另一個一次性密鑰或另一個一次性認證碼，該第二控制規範包含另一個一次性存取規範及另一個一次性指令規範之至少一者。該一次性動態連結程式產生單元 13 還用以根據該第二認證資料及該第二控制規範產生一第二一次性動態連結程式，該保護單元 15 將該第二一次性動態連結程式傳送給執行於該作業系統 311 中的合法應用程式 5，此時表示該

合法應用程式 5 又轉換爲待比對應用程式，繼而該認證單元 14 接收該待比對應用程式的該第二認證資料以對該待比對應用程式進行再次認證，且該待比對應用程式接收該認證單元 14 的該第二認證資料以對該認證單元 14 進行再次認證。

【0022】 以下將配合圖 2~3 流程圖來說明本發明應用程式存取保護方法之較佳實施例以及該應用程式存取保護裝置 1 之各元件的細節，並將步驟歸納成一認證過程及一再認證過程。

【0023】 參閱圖 1 與圖 2，本發明應用程式存取保護方法之認證過程包含下列步驟，其中該合法應用程式 5 儲存於該儲存裝置 4 之保護區 41 內，該作業系統 311 無法對該保護區 41 內的合法應用程式 5 進行刪除與寫入。

【0024】 如步驟 601 所示，當該作業系統 311 從該儲存裝置 4 之保護區 41 內讀取該合法應用程式 5 及其對應的該預設一次性動態連結程式時，該認證資料產生單元 11 產生該第一認證資料，該控制規範產生單元 12 產生該第一控制規範，且該一次性動態連結程式產生單元 13 根據該第一認證資料及該第一控制規範產生該第一一次性動態連結程式，該保護單元 15 將該第一一次性動態連結程式傳送給執行於該作業系統 311 中的合法應用程式 5，以取代該預設一次性動態連結程式。在本較佳實施例中，該合法應用程式 5 及該預設一次性動態連結程式屬於兩個分開的檔案，該作業系統 311 可分別讀取該合法應用程式 5 及該第一一次性

動態連結程式，亦即先讀取該合法應用程式 5，再讀取該取代該預設一次性動態連結程式的第一一次性動態連結程式。然而，在其他實施例中，該合法應用程式 5 及對應的預設一次性動態連結程式屬於同一個檔案，亦即，該合法應用程式 5 包含該應用子程式及該預設一次性動態連結程式，該作業系統 311 即無法分別讀取該合法應用程式 5 及該第一一次性動態連結程式，而須待該預設一次性動態連結程式已被該第一一次性動態連結程式取代後，再讀取該包含該應用子程式及該第一一次性動態連結程式的合法應用程式 5。

【0025】 如步驟 602 所示，該合法應用程式 5 根據該第一一次性動態連結程式產生該第一認證資料及該第一控制規範。

【0026】 值得特別說明的是，由於該作業系統 311 可能存在安全漏洞，因此該合法應用程式 5 可能在被讀取到作業系統 311 的過程中被竄改爲非法應用程式。因此執行於作業系統 311 中的應用程式須先經過認證才可控制該受控裝置 2，故執行於作業系統 311 中的應用程式將被視爲待比對應用程式。

【0027】 如步驟 603 所示，該認證單元 14 判定執行於該作業系統 311 中之待比對應用程式是否具有該第一認證資料及第一控制規範，若是，則繼續進行步驟 605；否則，進行步驟 604。

【0028】 如步驟 604 所示，該待比對應用程式爲無法被

授權之非法應用程式，且該應用程式存取保護裝置 1 不允許該非法應用程式控制該受控裝置 2。

【0029】 如步驟 605 所示，該認證單元 14 接收該待比對應用程式的第一認證資料以對該待比對應用程式進行認證，且該待比對應用程式接收該認證單元 14 的第一認證資料以對該應用程式存取保護裝置 1 之認證單元 14 進行認證，其中該認證單元 14 的第一認證資料為該認證資料產生單元 11 所產生的第一認證資料。

【0030】 如步驟 606 所示，當該認證單元 14 與該待比對應用程式完成彼此間的雙向認證後，表示該待比對應用程式即為該合法應用程式 5，且該合法應用程式 5 將該符合該第一控制規範的指令以該合法應用程式 5 的第一認證資料加密後傳送至該處理單元 16。

【0031】 如步驟 607 所示，該認證單元 14 啓動該處理單元 16，使該處理單元 16 接收該加密後的指令且根據該第一認證資料解密該指令。

【0032】 如步驟 608 所示，該處理單元 16 根據該解密後的指令控制該受控裝置 2，藉以使得該合法應用程式 5 可經由該處理單元 16 控制該受控裝置 2。

【0033】 參閱圖 1 與圖 3，再次認證過程的使用情境可有多種模式，例如，可設計為當該合法應用程式 5 要再次傳送指令以控制該受控裝置 2 時，即啓動再次認證過程，亦可設計為當該合法應用程式 5 傳送特定指令以控制該受控裝置 2 時，即啓動再次認證過程，或是設計為在每經過一

時間區間就啓動再次認證過程，可依使用需求的不同而設計不同的使用情境。再次認證過程可更進一步地避免當該合法應用程式 5 被置換或竄改爲非法應用程式時，卻沒有被發現，而使非法應用程式控制該受控裝置 2，此外再次認證過程亦可變更該應用程式存取保護裝置 1 與合法應用程式 5 之間的控制規範。以下將詳細說明本發明應用程式存取保護方法之再次認證過程所包含的步驟。

【0034】 如步驟 701 所示，該認證資料產生單元 11 產生該第二認證資料，該控制規範產生單元 12 產生該第二控制規範，且該一次性動態連結程式產生單元 13 根據該第二認證資料及該第二控制規範產生該第二一次性動態連結程式，該保護單元 15 將該第二一次性動態連結程式傳送給執行於該作業系統 311 中的合法應用程式 5，以取代該第一一次性動態連結程式。

【0035】 如步驟 702 所示，該合法應用程式 5 根據該第二一次性動態連結程式產生該第二認證資料及該第二控制規範。

【0036】 值得特別說明的是，由於執行於作業系統 311 中的應用程式須先經過再次認證才可控制該受控裝置 2，故執行於作業系統 311 中的應用程式將再度被視爲待比對應用程式。

【0037】 如步驟 703 所示，該認證單元 14 判定執行於該作業系統 311 中之待比對應用程式是否具有該第二認證資料及第二控制規範，若是，則繼續進行步驟 705；否則，進

行步驟 704。

【0038】 如步驟 704 所示，該待比對應用程式爲無法被授權之非法應用程式，且該應用程式存取保護裝置 1 不允許該非法應用程式控制該受控裝置 2。

【0039】 如步驟 705 所示，該認證單元 14 接收該待比對應用程式的該第二認證資料以對該待比對應用程式進行認證，且該待比對應用程式接收該認證單元 14 的該第二認證資料以對該應用程式存取保護裝置 1 之認證單元 14 進行認證，其中該認證單元 14 的第二認證資料爲該認證資料產生單元 11 所產生的第二認證資料。

【0040】 如步驟 706 所示，當該認證單元 14 與該待比對應用程式完成彼此間的雙向認證後，表示該待比對應用程式即爲該合法應用程式 5，且該合法應用程式 5 將另一符合該第二控制規範的指令以該合法應用程式 5 的第二認證資料加密後傳送至該處理單元 16。

【0041】 如步驟 707 所示，該認證單元 14 啓動該處理單元 16，使該處理單元 16 接收該加密後的另一指令且根據該第二認證資料解密該另一指令。

【0042】 如步驟 708 所示，該處理單元 16 根據該解密後的另一指令控制該受控裝置 2，藉以使得該合法應用程式 5 可經由該處理單元 16 控制該受控裝置 2。

【0043】 綜上所述，藉由將該合法應用程式 5 儲存於該儲存裝置 4 之保護區 41 內，使得不論是作業系統 311 或惡意程式皆無法對該保護區 41 內的合法應用程式 5 進行刪除

與寫入，因此，該合法應用程式 5 僅可能在運行於作業系統 311 時會被仿冒、竄改或植入惡意程式，然而藉由該保護單元 15 將該第一一次性動態連結程式傳送給執行於該作業系統 311 中的合法應用程式 5，使得當運行於該作業系統 311 中的合法應用程式 5 被仿冒、竄改或植入惡意程式後，即不具該第一一次性動態連結程式，而無法通過該認證單元 14 的認證，因此，只有具有該第一認證資料及第一控制規範的合法應用程式 5 才能控制該受控裝置 2，故確實能達成本發明之目的。

【0044】 惟以上所述者，僅爲本發明之較佳實施例而已，當不能以此限定本發明實施之範圍，即大凡依本發明申請專利範圍及專利說明書內容所作之簡單的等效變化與修飾，皆仍屬本發明專利涵蓋之範圍內。

【符號說明】

【0045】

1 ····· 應用程式存取保護裝置

11 ····· 認證資料產生單元

12 ····· 控制規範產生單元

13 ····· 一次性動態連結程式產生單元

14 ····· 認證單元

15 ····· 保護單元

16 ····· 處理單元

2 ····· 受控裝置

3 ····· 主機板

31 ····· 主記憶體

311····· 作業系統

32 ····· 中央處理單元

4 ····· 儲存裝置

41 ····· 保護區

42 ····· 隱藏區

5 ····· 合法應用程式

601~608· 步驟

701~708· 步驟

【生物材料寄存】

國內寄存資訊【請依：寄存機構、日期、號碼順序註記】

國外寄存資訊【請依：寄存國家、機構、日期、號碼順序註記】

【序列表】(請換頁單獨記載)

申請專利範圍

1. 一種應用程式存取保護方法，包含以下步驟：

(A)一具有一第一認證資料及一第一控制規範之應用程式存取保護裝置判定執行於一作業系統中之一待比對應用程式是否具有該第一認證資料及第一控制規範；及

(B)在該步驟(A)之判定結果爲否之情況下，表示該待比對應用程式爲一無法被授權之非法應用程式，且該應用程式存取保護裝置不允許該非法應用程式控制一受控裝置。

2. 如請求項 1 所述的應用程式存取保護方法，還包含在該步驟(A)之前的一步驟(C)，當該作業系統從一儲存裝置之一保護區內讀取一合法應用程式時，該應用程式存取保護裝置將該第一認證資料及第一控制規範傳送給執行於該作業系統中的合法應用程式，其中該作業系統無法對該保護區內的合法應用程式進行刪除與寫入。

3. 如請求項 2 所述的應用程式存取保護方法，其中在該步驟(C)中，該合法應用程式包含一應用子程式、一預設認證資料及一預設控制規範，當該作業系統從該儲存裝置之該保護區內讀取該合法應用程式時，該保護單元將該第一認證資料及第一控制規範傳送給執行於該作業系統中的合法應用程式以取代該預設認證資料及該預設控制規範。

4. 如請求項 2 所述的應用程式存取保護方法，其中在該步

驟(C)中，當該作業系統從該儲存裝置之該保護區內讀取該合法應用程式以及其對應的一預設認證資料及一預設控制規範時，該保護單元將該第一認證資料及第一控制規範傳送給執行於該作業系統中的合法應用程式。

5. 如請求項2所述的應用程式存取保護方法，還包含一步驟(D)，在該步驟(A)之判定結果爲是之情況下，表示該待比對應用程式即爲該合法應用程式，且該應用程式存取保護裝置允許該合法應用程式控制該受控裝置，其中該步驟(D)包括以下子步驟：

(D-1)該應用程式存取保護裝置接收該待比對應用程式的第一認證資料以對該待比對應用程式進行認證，且該待比對應用程式接收該應用程式存取保護裝置的第一認證資料以對該應用程式存取保護裝置進行認證；

(D-2)當該應用程式存取保護裝置與該待比對應用程式完成彼此間的雙向認證後，表示該待比對應用程式即爲該合法應用程式，且該合法應用程式根據該第一控制規範傳送一指令至該應用程式存取保護裝置；及

(D-3)該應用程式存取保護裝置根據該指令控制該受控裝置，藉以使得該合法應用程式可經由該應用程式存取保護裝置，控制該受控裝置。

6. 如請求項5所述的應用程式存取保護方法，其中在該步驟(D-2)中，當該應用程式存取保護裝置與該合法應用程式完成彼此間的雙向認證後，該合法應用程式將該指令以該合法應用程式的第一認證資料加密後傳送至該應

用程式存取保護裝置，繼而在該步驟(D-3)中，該應用程式存取保護裝置再接收該加密後的指令且根據該應用程式存取保護裝置的第一認證資料解密該指令，且該應用程式存取保護裝置根據該解密後的指令控制該受控裝置，藉以使得該合法應用程式可經由該應用程式存取保護裝置，控制該受控裝置。

7. 如請求項5所述的應用程式存取保護方法，在該步驟(D)之後，還包含一再次認證步驟(E)，其中該步驟(E)包括以下子步驟：

(E-1)該應用程式存取保護裝置將一第二認證資料及一第二控制規範傳送給執行於該作業系統中的合法應用程式，且該執行於該作業系統中的合法應用程式又轉變爲該待比對應用程式；及

(E-2)該應用程式存取保護裝置接收該待比對應用程式的該第二認證資料以對該待比對應用程式進行再次認證，且該待比對應用程式接收該應用程式存取保護裝置的該第二認證資料以對該應用程式存取保護裝置進行再次認證。

8. 如請求項5所述的應用程式存取保護方法，其中，在該步驟(A)中，該第一控制規範包含一個一次性存取規範及一個一次性指令規範之至少一者，其中該一次性存取規範係爲該合法應用程式傳送該指令至該應用程式存取保護裝置的存取規範，該一次性指令規範係爲該應用程式存取保護裝置與該合法應用程式對該指令的編碼

規範。

9. 如請求項 8 所述的應用程式存取保護方法，其中，在該步驟(A)中，該第一控制規範的一次性存取規範包括該合法應用程式傳送該指令至該處理單元以存取該儲存裝置之一隱藏區的存取規範，其中該隱藏區無法被該作業系統辨識、讀取與寫入。

10. 如請求項 1 所述的應用程式存取保護方法，其中，在該步驟(A)中，該第一認證資料包含一個一次性認證演算法、一個一次性密鑰或一個一次性認證碼。

11. 一種應用程式存取保護裝置，介於該受控裝置與一作業系統之間，且適用於判定是否允許執行於該作業系統中的一待比對應用程式控制一受控裝置，該應用程式存取保護裝置包含：

一認證資料產生單元，用以產生一第一認證資料；

一控制規範產生單元，用以產生一第一控制規範；及

一認證單元，用以判定執行於該作業系統中之待比對應用程式是否具有該第一認證資料及第一控制規範，若判定結果爲否，表示該待比對應用程式爲一無法被授權之非法應用程式，且該認證單元不允許該非法應用程式控制該受控裝置。

12. 如請求項 11 所述的應用程式存取保護裝置，還包含一保護單元，當該作業系統從一儲存裝置之一保護區內讀取一合法應用程式時，該保護單元用以將該第一認證資

料及第一控制規範傳送給執行於該作業系統中的合法應用程式，其中該作業系統無法對該保護區內的合法應用程式進行刪除與寫入。

13. 如請求項 12 所述的應用程式存取保護裝置，其中該合法應用程式包含一應用子程式、一預設認證資料及一預設控制規範，當該作業系統從該儲存裝置之該保護區內讀取該合法應用程式時，該保護單元將該第一認證資料及第一控制規範傳送給執行於該作業系統中的合法應用程式以取代該預設認證資料及該預設控制規範。

14. 如請求項 12 所述的應用程式存取保護裝置，其中當該作業系統從該儲存裝置之該保護區內讀取該合法應用程式以及其對應的一預設認證資料及一預設控制規範時，該保護單元將該第一認證資料及第一控制規範傳送給執行於該作業系統中的合法應用程式。

15. 如請求項 12 所述的應用程式存取保護裝置，還包含一處理單元，若該認證單元的判定結果爲是，該認證單元接收該待比對應用程式的第一認證資料以對該待比對應用程式進行認證，該待比對應用程式接收該認證單元的第一認證資料以對該應用程式存取保護裝置進行認證，當該認證單元與該待比對應用程式完成彼此間的雙向認證後，表示該待比對應用程式即爲該合法應用程式，且該認證單元啓動該處理單元，使該處理單元接收該合法應用程式根據該第一控制規範所傳送的一指令，繼而該處理單元根據該指令控制該受控裝置，藉以使得該

合法應用程式可經由該處理單元，控制該受控裝置。

16. 如請求項 15 所述的應用程式存取保護裝置，其中當該認證單元與該合法應用程式完成彼此間的雙向認證後，該合法應用程式將該指令以該合法應用程式的第一認證資料加密後傳送至該處理單元，該處理單元再接收該加密後的指令且根據該第一認證資料解密該指令，繼而該處理單元根據該解密後的指令控制該受控裝置，藉以使得該合法應用程式可經由該處理單元，控制該受控裝置。

17. 如請求項 15 所述的應用程式存取保護裝置，其中該認證資料產生單元還用以產生一第二認證資料，該控制規範產生單元還用以產生一第二控制規範，該保護單元將該第二認證資料及該第二控制規範傳送給執行於該作業系統中的合法應用程式，且該執行於該作業系統中的合法應用程式又轉變爲該待比對應用程式，繼而該認證單元接收該待比對應用程式的該第二認證資料以對該待比對應用程式進行再次認證，且該待比對應用程式接收該認證單元的該第二認證資料以對該認證單元進行再次認證。

18. 如請求項 15 所述的應用程式存取保護裝置，其中該第一控制規範包含一個一次性存取規範及一個一次性指令規範之至少一者，其中該一次性存取規範係爲該合法應用程式傳送該指令至該處理單元的存取規範，該一次性指令規範係爲該處理單元與該合法應用程式對該指

令的編碼規範。

19. 如請求項 18 所述的應用程式存取保護裝置，其中該第一控制規範的一次性存取規範包括該合法應用程式傳送該指令至該處理單元以存取該儲存裝置之一隱藏區的存取規範，其中該隱藏區無法被該作業系統辨識、讀取與寫入。

20. 如請求項 11 所述的應用程式存取保護裝置，其中該第一認證資料包含一個一次性認證演算法、一個一次性密鑰或一個一次性認證碼。

圖式

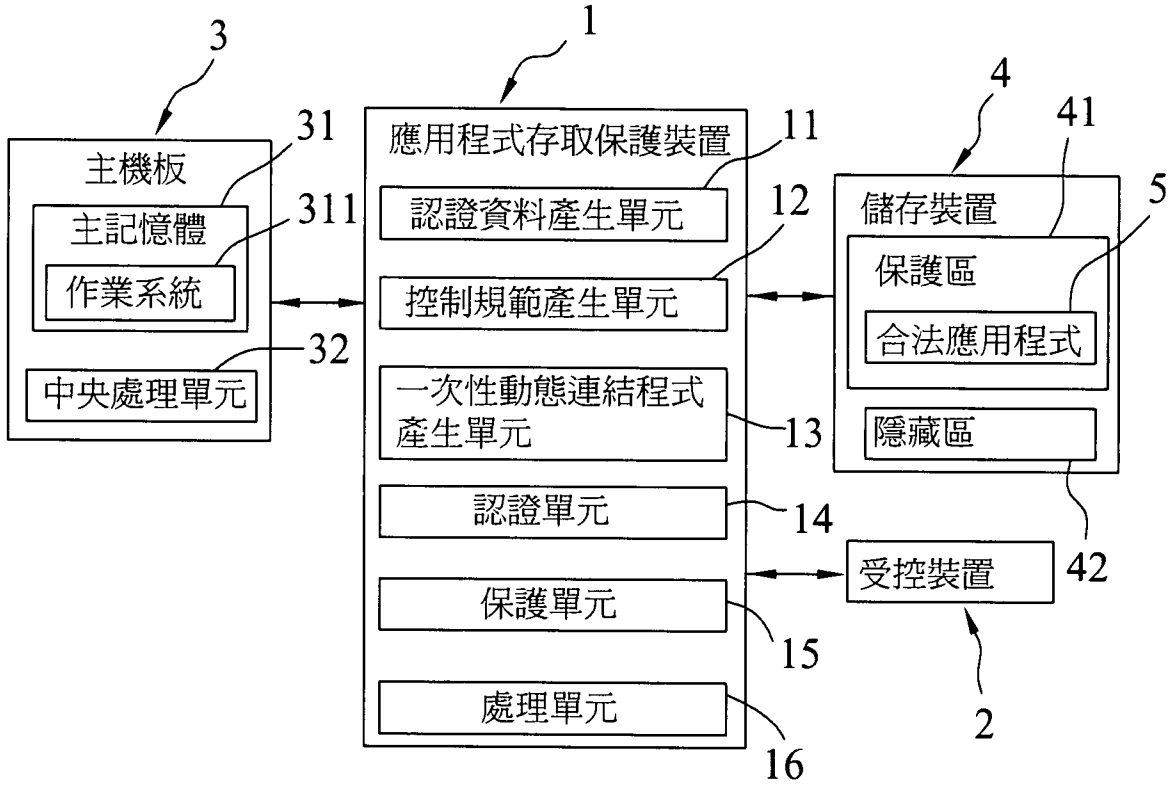
3
1
4
31
應用程式存取保護裝置
11
41
主機板
認證資料產生單元
5
311
12
儲存裝置
主記憶體
保護區
作業系統
控制規範產生單元
合法應用程式
32
一次性動態連結程式
產生單元
13
隱藏區
認證單元
14
42
受控裝置
保護單元
15
中央處理單元
處理單元
2
16

圖1

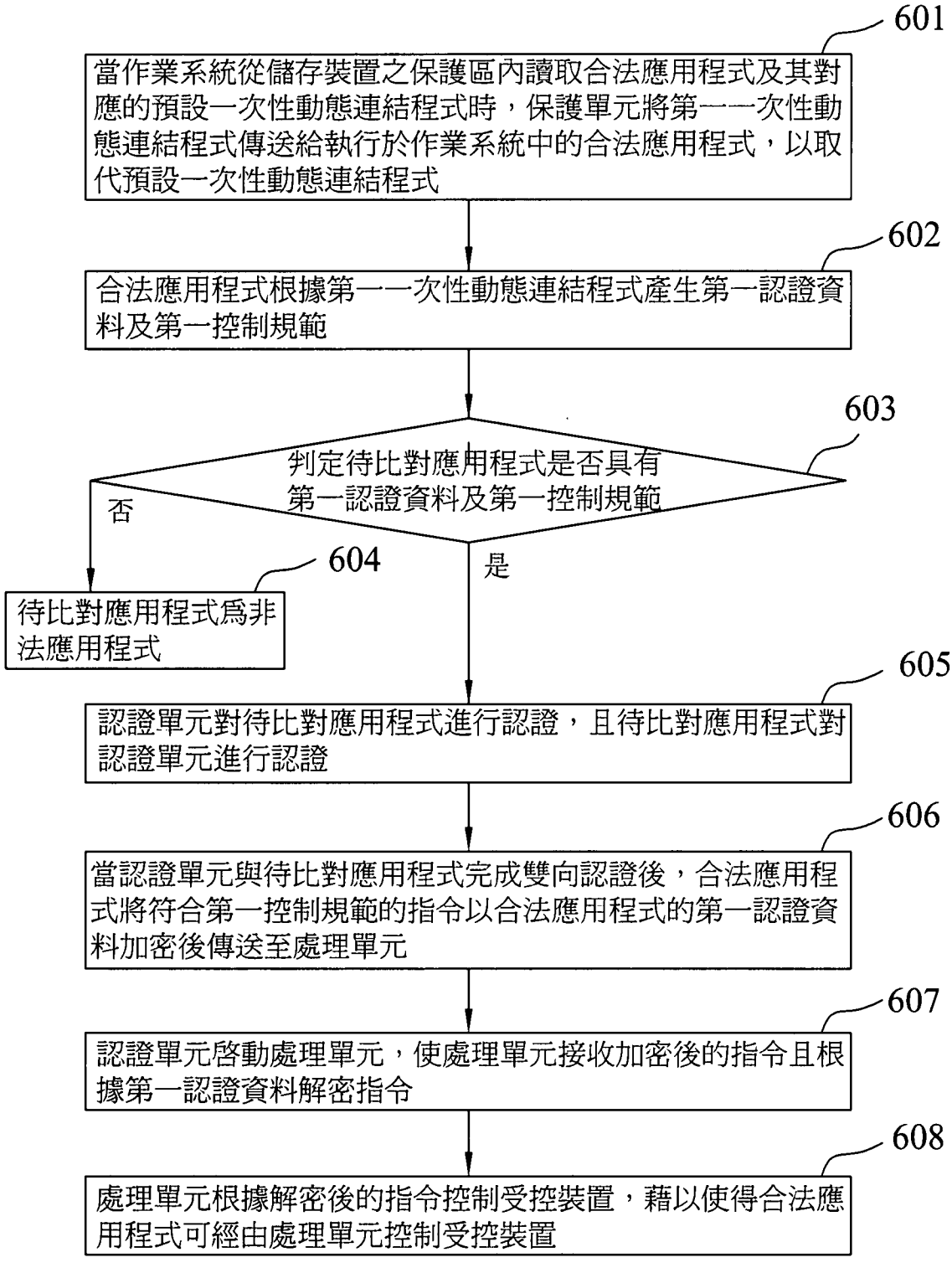
601
當作業系統從儲存裝置之保護區內讀取合法應用程式及其對應的預設一次性動態連結程式時，保護單元將第一一次性動態連結程式傳送給執行於作業系統中的合法應用程式，以取代預設一次性動態連結程式
602
合法應用程式根據第一一次性動態連結程式產生第一認證資料及第一控制規範
603
判定待比對應用程式是否具有第一認證資料及第一控制規範
否
是
604
待比對應用程式爲非法應用程式
605
認證單元對待比對應用程式進行認證，且待比對應用程式對認證單元進行認證
606
當認證單元與待比對應用程式完成雙向認證後，合法應用程式將符合第一控制規範的指令以合法應用程式的第一認證資料加密後傳送至處理單元
607
認證單元啓動處理單元，使處理單元接收加密後的指令且根據第一認證資料解密指令
608
處理單元根據解密後的指令控制受控裝置，藉以使得合法應用程式可經由處理單元控制受控裝置

圖2

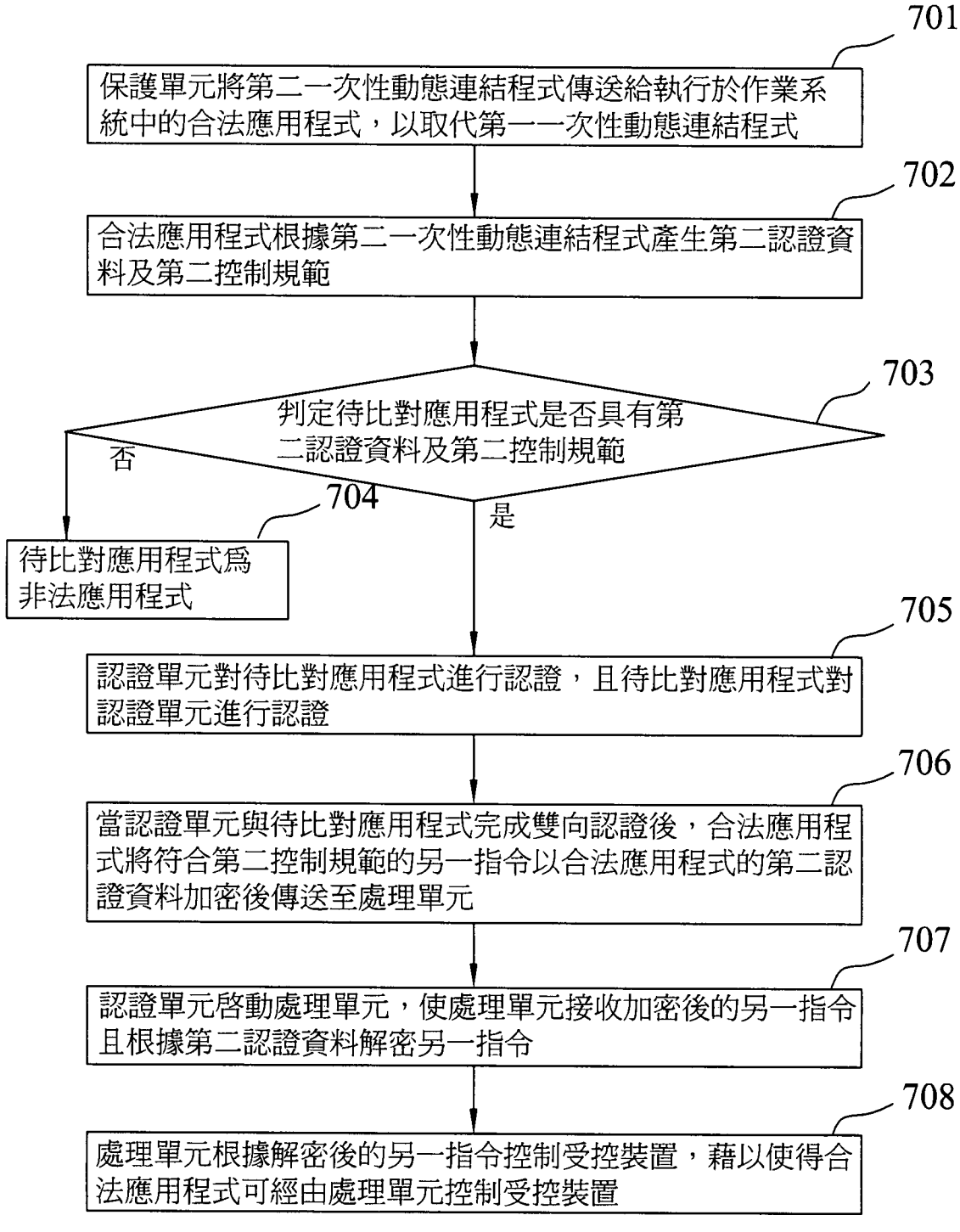
701
保護單元將第二一次性動態連結程式傳送給執行於作業系統中的合法應用程式，以取代第一一次性動態連結程式
702
合法應用程式根據第二一次性動態連結程式產生第二認證資料及第二控制規範
703
判定待比對應用程式是否具有第二認證資料及第二控制規範
否
是
704
待比對應用程式爲非法應用程式
705
認證單元對待比對應用程式進行認證，且待比對應用程式對認證單元進行認證
706
當認證單元與待比對應用程式完成雙向認證後，合法應用程式將符合第二控制規範的另一指令以合法應用程式的第二認證資料加密後傳送至處理單元
707
認證單元啓動處理單元，使處理單元接收加密後的另一指令且根據第二認證資料解密另一指令
708
處理單元根據解密後的另一指令控制受控裝置，藉以使得合法應用程式可經由處理單元控制受控裝置

圖3