201717088

(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 201717088 A

(43)公開日： 中華民國 106 (2017) 年 05 月 16 日

(21)申請案號：105132994 (22)申請日： 中華民國 105 (2016) 年 10 月 13 日

(51)Int. Cl.： *G06F21/56 (2013.01)*

(30)優先權：2015/11/09 美國 14/935,522

(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)
美國

(72)發明人：阿哈馬札迪 席也阿里 AHMADZADEH, SEYED ALI (CA)；伊斯萊 那依姆 ISLAM, NAYEEM (US)；克里斯多朵瑞庫 祕海 CHRISTODORESCU, MIHAI (US)；庫伯塔 拉嘉爾許 GUPTA, RAJARSHI (US)；達斯 紹米特拉莫漢 DAS, SAUMITRA MOHAN (IN)

(74)代理人：李世章

申請實體審查：無 申請專利範圍項數：30 項 圖式數：7 共 62 頁

(54)名稱

動態蜜罐系統

DYNAMIC HONEYPOT SYSTEM

(57)摘要

各個實施例包括配置為使用行為分析演算法和動態資源提供觸發惡意應用程式的惡意活動的蜜罐系統。一種由計算設備的處理器執行的方法（該計算設備可以是行動計算設備）可以包括以下步驟：至少部分地基於分析決定當前執行在該計算設備上的目標應用程式是否是潛在地具有惡意的，預測該目標應用程式的觸發條件作為對決定該目標應用程式潛在地具有惡意的回應，至少部分地基於該預測的觸發條件提供一或多個資源，監聽該目標應用程式對應於所提供的一或多個資源的活動，並且至少部分地基於該等監聽的活動決定該目標應用程式是否為惡意應用程式。該等資源可以是設備部件（例如，網路介面、感測器等等）及/或資料（例如，檔案等）。

Various embodiments include a honeypot system configured to trigger malicious activities by malicious applications using a behavioral analysis algorithm and dynamic resource provisioning. A method performed by a processor of a computing device, which may be a mobile computing device, may include determining whether or not a target application currently executing on the computing device is potentially malicious based, at least in part, on the analysis, predicting a triggering condition of the target application in response to determining the target application is potentially malicious, provisioning one or more resources based, at least in part, on the predicted triggering condition, monitoring activities of the target application corresponding to the provisioned one or more resources, and determining whether or not the target application is a malicious application based, at least in part, on the monitored activities. The resources may be device components (e.g., network interface(s), sensor(s), etc.) and/or data (e.g., files, etc.).

指定代表圖：

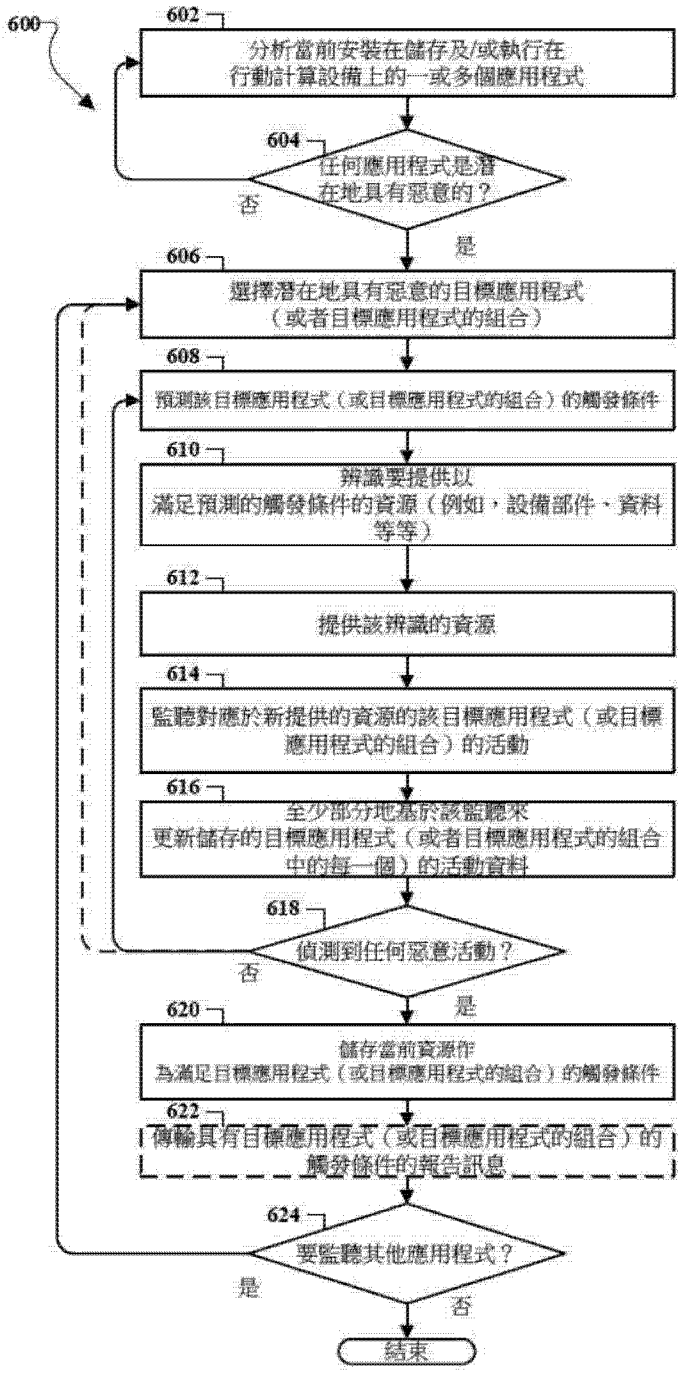

圖6

符號簡單說明：

600・・・方法

602・・・方塊

604・・・判定方塊

606・・・方塊

608・・・方塊

610・・・方塊

612・・・方塊

614・・・方塊

616・・・方塊

618・・・判定方塊

620・・・方塊

622・・・可選方塊

624・・・判定方塊

201717088
專利案號：105132994
201717088
E 申請日：105/10/13
I IPC分類：G06F21/56(2013.01)

【發明摘要】

【中文發明名稱】動態蜜罐系統

【英文發明名稱】DYNAMIC HONEYPOT SYSTEM

【中文】

各個實施例包括配置為使用行為分析演算法和動態資源提供觸發惡意應用程式的惡意活動的蜜罐系統。一種由計算設備的處理器執行的方法（該計算設備可以是行動計算設備）可以包括以下步驟：至少部分地基於分析決定當前執行在該計算設備上的目標應用程式是否是潛在地具有惡意的，預測該目標應用程式的觸發條件作為對決定該目標應用程式潛在地具有惡意的回應，至少部分地基於該預測的觸發條件提供一或多個資源，監聽該目標應用程式對應於所提供的一或多個資源的活動，並且至少部分地基於該等監聽的活動決定該目標應用程式是否為惡意應用程式。該等資源可以是設備部件（例如，網路介面、感測器等等）及/或資料（例如，檔案等）。

【英文】

Various embodiments include a honeypot system configured to trigger malicious activities by malicious applications using a behavioral analysis algorithm and dynamic resource provisioning. A method performed by a processor of a computing device, which may be a mobile computing device, may include determining whether or not a target application currently executing on the computing device is potentially malicious based, at least in part, on the analysis, predicting a triggering condition of the target application in response to

determining the target application is potentially malicious, provisioning one or more resources based, at least in part, on the predicted triggering condition, monitoring activities of the target application corresponding to the provisioned one or more resources, and determining whether or not the target application is a malicious application based, at least in part, on the monitored activities. The resources may be device components (e.g., network interface(s), sensor(s), etc.) and/or data (e.g., files, etc.).

【指定代表圖】第（ 6 ）圖。

【代表圖之符號簡單說明】

6 0 0 方 法

6 0 2 方 塊

6 0 4 判 定 方 塊

6 0 6 方 塊

6 0 8 方 塊

6 1 0 方 塊

6 1 2 方 塊

6 1 4 方 塊

6 1 6 方 塊

6 1 8 判 定 方 塊

6 2 0 方 塊

6 2 2 可 選 方 塊

6 2 4 判 定 方 塊

【特徵化學式】

無

【發明說明書】

【中文發明名稱】動態蜜罐系統

【英文發明名稱】DYNAMIC HONEYPOT SYSTEM

【技術領域】

【0001】 本發明係關於動態蜜罐系統。

【先前技術】

【0002】 「蜜罐系統」（或簡稱「蜜罐」）是有目的地被部署以用於由惡意軟體探測、攻擊和盜用，以便發現、辨識和特徵化此種軟體的電腦系統。典型的蜜罐系統被鎖住以便將惡意軟體限制在該系統的控制的功能，而不會使該惡意軟體能夠發出進一步的、不可控制的攻擊。典型的蜜罐系統是能夠進行廣泛的系統和應用程式監聽和登錄的。蜜罐系統經常很容易被惡意軟體經由網路存取（例如，在區域網路（LAN）上是可探索的等等）。蜜罐系統的監聽和控制功能被很好地偽裝以避免被配置為辨識和避免蜜罐的惡意軟體偵測到。有了該等特性，蜜罐系統經常用於在網路中吸引或隔離攻擊，以及用於產生指示惡意軟體如何操作的有用資料。例如，蜜罐系統能夠提供指示惡意軟體形成的潛在威脅的資料，該資料能夠與其他設備共享以便用作早期預警系統。大體而言，成功的蜜罐系統提供受控制的時機以向惡意軟體學習而不用擔心對資料、網路和該網路上的計算設備的實際損害。

【發明內容】

【0003】 各個實施例提供用於觸發應用程式的惡意活動的蜜罐系統的方法、設備、系統和非暫時性處理器可讀取儲存媒體。各個實施例方法可以由實現該蜜罐系統的計算設備的處理器執行。實現各個實施例的計算設備可以是行動計算設備。各個實施例可以包括預測一或多個目標應用程式的觸發條件，作為對決定該一或多個目標應用程式潛在地具有惡意的回應。各個實施例亦可以包括至少部分地基於該預測的觸發條件提供一或多個資源，並且監聽該一或多個目標應用程式對應於所提供的一或多個資源的活動。各個實施例亦可以包括至少部分地基於所監聽到的活動決定該一或多個目標應用程式是否是具有惡意的。一些實施例亦可以包括決定當前在該計算設備上執行的應用程式是否是潛在地具有惡意的，並且指定該應用程式作為一或多個目標應用程式之一作為對決定該應用程式潛在地具有惡意的回應。在一些實施例中，決定當前在該計算設備上執行的應用程式是否是潛在地具有惡意的可以包括分析該對應於對該計算設備的資源的存取的對一或多個目標應用程式的許可中的至少一個。在一些實施例中，決定當前執行在該計算設備上的應用程式是否是潛在地具有惡意的可以包括分析儲存的指示一或多個目標應用程式的先前活動的活動資料。

【0004】 在一些實施例中，該一或多個資源可以包括一或多個設備部件和資料之一或二者。在一些實施例中，該一或多個設備部件可以包括由已安裝應用程式、作業系

統、網路介面、處理單元、資料儲存單元、耦合的設備、輸出單元、輸入單元和感測器組成的群組中的至少一個成員。在一些實施例中，該資料可以包括由連絡人清單、儲存的檔案、個人資訊、網路狀況資料、訂閱資訊、位置資訊、系統資訊、已知易受攻擊資訊和感測器資料組成的群組的至少一個成員。

【0005】 在一些實施例中，預測該一或多個目標應用程式的該觸發條件可以包括評估對該一或多個目標應用程式的許可、先前對於該一或多個目標應用程式可存取的任何資源和儲存的指示該一或多個目標應用程式的先前活動的活動資料中的至少一個。

【0006】 在一些實施例中，至少部分地基於該預測的觸發條件提供該一或多個資源可以包括至少部分地基於該預測的觸發條件調整先前對於該一或多個目標應用程式可見的資源。在一些實施例中，至少部分地基於該預測的觸發條件提供該一或多個資源可以包括配置先前對於該一或多個目標應用程式不可見的資源使該資源變得對於該一或多個目標應用程式可見。在一些實施例中，至少部分地基於該預測的觸發條件提供該一或多個資源可以包括至少部分地基於該預測的觸發條件建立虛擬資源，其中該虛擬資源代表並非實際存在於該計算設備中或由該計算設備支援的模仿的設備部件或資料。

【0007】 在一些實施例中，監聽對應於該提供的一或多個資源的該一或多個目標應用程式的活動可以包括偵測

該一或多個目標應用程式進行的應用程式介面（API）呼叫。在一些實施例中，至少部分地基於該等監聽的活動決定該一或多個目標應用程式是否是具有惡意的可以包括評估該等監聽到的活動和儲存的指示該一或多個目標應用程式的先前活動的活動資料。

【0008】 一些實施例亦可以包括更新儲存的該一或多個目標應用程式的活動資料，該活動資料包括關於在監聽的該一或多個目標應用程式的活動導致決定該一或多個目標應用程式是具有惡意的時提供的資源的資訊。一些實施例可以亦包括傳輸指示該一或多個目標應用程式的該觸發條件的報告訊息，作為對決定該一或多個目標應用程式具有惡意的回應。

【0009】 其他實施例包括配置有用於執行上文描述的方法的操作的處理器可執行指令的計算設備。其他實施例包括非暫時性處理器可讀取媒體，非暫時性處理器可讀取媒體上儲存有處理器可執行指令，配置為使計算設備執行上文描述的方法的操作。其他實施例包括一種系統，該系統包括配置有用於執行上述方法的操作的處理器可執行指令的計算設備。

【圖式簡單說明】

【0010】 合併在本案中的並且組成此說明書的一部分的附圖圖示各個實施例，並且與上文提供的一般描述和下文提供的詳細描述一起用於解釋說明請求項的特徵。

【0011】 圖1是根據各種實施方式包括配置為用作蜜罐系統的行動計算設備的系統示意圖。

【0012】 圖2-圖5是根據各種實施方式圖示與配置為用作蜜罐系統的行動計算設備的資源相關聯的動態資料的示意圖。

【0013】 圖6是根據各種實施方式用於由計算設備蜜罐執行動態提供資源的操作以便吸引或激起應用程式的惡意活動的方法的程序流程圖。

【0014】 圖7是適合用於一種實現中的行動計算設備的部件方塊圖。

【實施方式】

【0015】 下文將參照附圖詳細描述各個實施例和實施方式。相同的元件符號將會在貫穿附圖中儘可能地用於引用相同或相似的部分。針對特定實例和實施方式進行的參考是為了解釋說明的目的，而非意在限制實施方式或請求項的範疇。

【0016】 各個實施例和實施方式包括在計算設備中產生實體的動態蜜罐系統，該動態蜜罐系統被配置為經由以預測的引出惡意行為的方式向應用程式呈現資源和功能的各種組合，從而辨識處理器上執行的應用程式的惡意行為。該計算設備可以是但並不僅限於行動計算設備。針對每個潛在的惡意應用程式，該蜜罐系統可以觀察該應用程式的活動和狀態並且使用觀察到的資料執行分析。該蜜罐系統可以預測諸如可用的設備功能性和該系統的操作狀

態之類的狀況，該等狀況是使每個潛在惡意應用程式執行惡意動作可能需要的。該蜜罐系統可以相應地提供資源，諸如經由使各種設備部件（例如，感測器、網路介面、記憶體位置、處理器、無線電單元等等）及/或資料（例如，連絡人清單、檔案、訊息內容等等）可存取或可見。該蜜罐系統可以繼續監聽潛在的惡意應用程式並反覆運算地調整可用資源，直到該潛在惡意應用程式展現出惡意活動為止。經由使行動計算設備（諸如智慧型電話）中常見的設備部件可存取或可見，各種實施例和實施方式可以用作評估可能將行動計算設備的常見檔案和功能用於惡意目的的應用程式的行動蜜罐系統。

【0017】 術語「計算設備」在本案中用於代表配備有至少一個處理器的電子設備。計算設備的實例可以包括行動計算設備（例如，蜂巢式電話、可穿戴設備、智慧型電話、網路pad、平板電腦、網際網路功能的蜂巢式電話、Wi-Fi功能的電子設備、個人數位助理（PDA）、膝上型電腦等等）、個人電腦和伺服器計算設備。例如，行動計算設備可以包括異構的或同種類的多核智慧型電話。在各種實施方式中，計算設備可以配置有記憶體及/或儲存以及網路功能，諸如被配置為建立廣域網路（WAN）連接（例如，蜂巢網路連接等等）及/或區域網路（LAN）連接（例如，經由Wi-Fi路由器的到網際網路的有線/無線連接等等）的網路收發機和天線。

【0018】 術語「惡意行為」、「惡意活動」和「惡意動作」在本案中交替使用，用於代表由計算設備上執行的應用程式（例如，惡意軟體）執行的可能針對該計算設備及/或相關聯的使用者導致攻擊、危害、失敗、資料丟失及/或其他不需要的或未授權的狀況的任意一或多個操作。例如，惡意活動可以包括未授權或不需要的資料存取（例如，讀取、複製等等）、資料傳輸（例如，向遠端設備轉移的敏感性資料等等）及/或資料交換（例如，重命名、寫、覆寫、刪除、損壞、加密、解密、改變許可等等）。舉另一個實例，惡意活動可以包括未授權的或不需要的設備部件變化，諸如重啟系統或子系統、處理器過載、停用感測器、斷開儲存設備連接等等。惡意活動可以包括僅在組合執行時才造成不需要的或未授權的結果的多個操作。例如，惡意活動可以包括典型的對耦合的外部儲存設備的良性輪詢與典型的對複製敏感性資料的良性請求的組合。

【0019】 有各種不同類型的典型蜜罐系統。「主動的」蜜罐系統可以被配置為監聽並回應從惡意應用程式偵測到的威脅。「被動的」蜜罐系統可以被配置為簡單地收集監聽資料（例如，偵測到的應用程式介面（API）呼叫等等）用於對採用和惡意活動的分析。一些蜜罐系統被設計為僅提供對特定惡意應用程式可能感興趣的計算系統的功能的存取。例如，一種蜜罐系統可以經由重新建立公知的易受攻擊的子系統而不是提供全功能的系統來將公知

的惡意軟體應用程式的活動作為目標。該等蜜罐系統技術可以將惡意應用程式的互動限制在公知的易受該特定惡意應用程式攻擊的子系統。其他蜜罐系統技術可以採用重新建立全功能系統的高互動設計，諸如經由以高管理負擔為代價來模仿一般特性和資源。

【0020】 由於需要資源以便為評估惡意活動提供適當環境，蜜罐系統通常實現在具有定義好的操作條件及/或設備部件的伺服器或靜態計算系統中。一些蜜罐系統亦可以實現在行動計算系統中，但是通常由於行動系統有限的處理能力、記憶體和功率而具有更小的範疇。例如，大量的或持續的監聽操作可能由於有限的電池壽命和處理馬力而難以在行動設備上在更長時間段完成。

【0021】 一些複雜的惡意應用程式能夠選擇性地決定何時攻擊計算系統以及決定用於攻擊的各種資源。例如，惡意軟體應用程式可以不顯露惡意活動（例如，從行動電話傳輸安全資料等）直到該惡意軟體應用程式被下載並安裝到系統上之後很久。舉另一個實例，該惡意軟體應用程式可以在執行時間的大部分內執行無害操作，僅在滿足主機計算系統的某些操作條件時才參與惡意活動（例如，刪除檔案等等）。不知道惡意活動何時可能發生或者何種資源可能被用於該等惡意活動，典型的蜜罐系統被迫採用代價很高的、對應用程式活動的持續監聽。

【0022】 一些惡意應用程式的複雜屬性是實現在行動計算設備上的蜜罐系統的另外的問題，因為行動設備通常

包括可以用於惡意活動的很大範圍的設備部件、功能和系統狀態。例如，行動電話上的惡意軟體應用程式可以利用或者依賴於多個通訊介面、大範圍的設備配置和操作場景（例如，可用的無線電存取技術、通道條件）、不同使用者行為（例如，提供輸入等等）和同時執行的應用程式的任意組合。惡意應用程式可以被設計為利用某些資源，使得惡意活動僅在給定的時間處滿足計算設備的高度專用和一套複雜操作條件時才被觸發。例如，惡意軟體可以使用智慧型電話的當前位置與一或多個其他因素組合以決定是否啟動惡意活動。行動系統中的惡意活動的如此多選擇使得蜜罐的設計很複雜，該等蜜罐能夠吸引並觸發該等惡意活動，從而留下該等流行的行動計算環境尤其易受攻擊。

【0023】 各個實施例提供使用因果分析及/或行為預測來觸發惡意應用程式的惡意活動的方法、設備和非暫時性處理器可讀取儲存媒體。大體而言，計算設備（例如，圖1中圖示的行動計算設備102）可以配置為用作蜜罐系統。在一個示例性實施方式中，該蜜罐系統可以是配置為在網路上可見的（例如，可探索的）的並且具有一些外部實體/使用者可用的受控制的功能的智慧型電話等等。蜜罐系統可以分析經由該計算設備的處理器（例如，圖1中的處理器121）執行的各個應用程式的各種特性、優先活動和許可。蜜罐系統亦可以監聽對該等應用程式的所有請求、訊息、輪詢、複製/寫入、存取和其他活動。至少部

分地基於該等分析和監聽，該蜜罐系統可以預測可以觸發該等應用程式的惡意活動的條件（例如，某些設備部件的存在、計算設備的系統狀態及/或其他操作條件）。隨後，該蜜罐系統可以提供新的資源並且繼續監聽以決定該等應用程式是否開始惡意地活動。該蜜罐系統可以反覆運算地繼續進行該等操作以便找到成功暴露惡意應用程式的資源的組合。有了至少部分地基於行為分析的該等預測，可以利用減少的系統監聽和偵測管理負擔來辨識出先前未知的威脅和弱點。

【0024】 在一些實施方式中，蜜罐系統可以使用機器學習演算法和應用程式的歷史活動資料來辨識潛在地具有惡意的應用程式。在一些實施方式中，應用程式可以至少部分地基於對該應用程式能夠或者被放置為發佈惡意活動的概率的計算被辨識為潛在地具有惡意的。例如，蜜罐系統可以至少部分地基於該應用程式的當前許可和先前觀察到的該應用程式的動作（例如，資料存取、連接請求等）的分析計算概率值。如此計算出的概率值可以與閾值比較，諸如至少部分地基於觀察到的與可疑的或潛在地具有惡意的活動匹配的動作隨著時間更新的預定義的閾值或動態閾值。

【0025】 使用潛在惡意應用程式的活動的分析，該蜜罐系統可以預測該潛在惡意應用程式要求在其將要顯現惡意活動之前出現在該行動計算設備上的條件（亦即，觸發條件）。例如，該蜜罐系統可以估計該潛在惡意應用程式

可以等待的網路條件（例如，信號強度、頻寬和連接類型）。該等估計的網路條件可以至少部分地基於在該計算設備的先前的操作條件內的該潛在惡意應用程式的記錄的動作，諸如當不同網路介面可用或不可用時。預測的觸發條件可以使該蜜罐系統能夠辨識可用於促使該潛在惡意應用程式開始動作的準確的資源（例如，啟用的設備部件、可用的網路介面等等）。此外，預測的觸發條件亦可以使該蜜罐系統辨識適當地誘騙該潛在惡意應用程式開始動作所要求的間接條件（例如，系統狀態、位置、配置參數等等）。

【0026】 該蜜罐系統可以提供辨識出的資源，諸如經由啟用設備部件及/或調整儲存的資料值。大體而言，提供可以包括停用、啟用、調整、配置、隱藏、顯示、建立、刪除及/或另外的使該行動計算設備的各種功能可用（或不可用）。提供的資源可以是獨立於該蜜罐系統的其他元件（例如，沙箱的）或由該蜜罐系統模仿的真實資源。提供的資源可以是對於應用程式的群組在系統範圍內可見的或者僅對潛在惡意應用程式可見。

【0027】 在一些實施方式中，提供的資源或其他相關資源可以被配置為向該潛在惡意應用程式隱藏該蜜罐系統的屬性。例如，當該蜜罐系統正在移動（或模擬移動）時，假的Wi-Fi存取點可以被辨識為來來回回。舉另一個實例，該蜜罐系統可以用多種不同的區域碼建立假的連絡人

清單以便類似於真實的連絡人清單一樣出現在實際使用者的智慧型電話上。

【0028】 在各種實施方式中，可以提供的資源可以由提供該蜜罐系統的計算設備的規範來決定或者不由其決定。例如，在一些實施方式中，該蜜罐系統可以被配置為調整及/或模仿沒有針對該計算設備實際出現或可用的功能（例如，全球定位系統（GPS）接收器、加速感測器、4G連接等等）。

【0029】 蜜罐系統可以密切地監聽並且分析對應於任何提供的資源的潛在惡意應用程式的活動。例如，該蜜罐系統可以截獲來自該潛在惡意應用程式的輸出訊息及/或應用程式介面（API）呼叫。

【0030】 若該潛在惡意應用程式不對應於具有惡意活動的提供的資源，則該蜜罐系統可以反覆運算地繼續至少部分地基於後續監聽/預測來預測觸發條件和提供新的（或調整的）資源。例如，該潛在惡意應用程式的活動的新的觀察可以被轉發給分析器以便辨識該潛在惡意應用程式等待使用的可能資源。舉另一個實例，作為對截獲來自該潛在惡意應用程式的輸出訊息及/或應用程式介面（API）呼叫的回應，該蜜罐系統可以用假的資訊進行回應（例如，可用的網路連接、連絡人清單資料、傳輸確認等等）。此反覆運算程序可以繼續針對該潛在惡意應用程式來定制該蜜罐系統的資源直到惡意活動被偵測到或者被完全分析。

【0031】 如前述，各個實施例的蜜罐系統在評估可能利用行動計算設備（諸如智慧型電話）的檔案、部件和功能的行動應用程式中尤其有用。由於此原因，各個實施例和實現是參考作為適用於實現實施例蜜罐系統的計算設備的實例的行動計算設備描述的。但是，對行動計算設備的參考僅僅是示例性的，而並不意在限制請求項的範疇。

【0032】 下文是根據各種實施方式在行動計算設備(例如，智慧型電話）上執行的蜜罐系統的非限制性實例。特定應用程式可以被設計為僅在該蜜罐系統位於烏克蘭時執行惡意活動（例如，洩漏密碼等等）。換言之，在位於烏克蘭之前，該應用程式將不會顯示任何惡意活動。該蜜罐系統可以觀察該應用程式具有對存取儲存的資料、廣域網路（WAN）連接和位置服務的許可。該資源可以是該蜜罐系統建立的實際資源或虛擬資源的任何組合。該蜜罐系統可以提供假的GPS座標，該等假的GPS座標指示該行動計算設備處於加州的三藩市。在一段週期內，該蜜罐系統可以觀察到該應用程式週期性地讀取或存取位置資料（例如，GPS資料），但是僅顯現有限的或良性的網路活動。

【0033】 至少部分地基於該等許可，該蜜罐系統可以推斷該應用程式有很高概率洩漏資訊。該蜜罐系統可以預測該應用程式可以要求特定位置來觸發惡意活動。作為回應，該蜜罐系統可以產生各種假的位置資料以指示在全世界的不同位置。當產生指示當前位置是在烏克蘭的位置資

料時，該應用程式可以被觸發並且可以開始執行洩漏敏感資訊的操作，因此確認該應用程式是具有惡意的。該蜜罐系統可以若有必要則阻止此洩漏並且可以將該等條件/可用的資源作為特定應用程式的準確觸發條件來記錄。

【0034】 在一些實施方式中，該蜜罐系統可以維護一段時間週期的所有應用程式的歷史和狀態，以便偵測具有延遲的或具體觸發器的惡意活動。在一些實施方式中，潛在惡意應用程式可以至少部分地基於後續活動被決定為不是具有惡意的。

【0035】 在各種實施方式中，可以由該蜜罐系統提供的資源可以包括各種設備部件（及/或相關聯的設置）和資料（及/或相關聯的設置）。例如，資源可以包括已安裝的應用程式（例如，病毒保護軟體、防火牆軟體等等）、作業系統（例如，安卓、Windows等等）、網路介面（用於在各種網路區域網路及/或廣域網路上建立通訊的硬體及/或軟體，諸如收發機、天線、控制器等等）、無線電存取技術（RAT）（例如，長期進化（LTE）、3G、2G、Wi-Fi、藍芽®等等）、處理單元（例如，數位信號處理器（DSP）、中央處理單元（CPU）、圖形處理單元（GPU）等等）、資料儲存單元（例如，記憶體、緩存、硬體驅動器等等）、耦合的設備（例如，經由通用序列匯流排（USB）連接的外部硬體驅動器、USB優盤、安全數位（SD）卡等等）、輸出單元（例如，顯示器、揚聲器等等）、輸入單元（例如，鍵盤、觸控式螢幕等等）及/或感測器（例

如，攝像機、麥克風、加速計、陀螺儀等等）的一或多個的任意組合。舉另一個實例，資源可以是資料，包括連絡人清單、儲存的檔案、安全或個人資訊（例如，圖片、視訊、保存的密碼、訊息內容、電子郵件等等）、網路狀況資料（例如，存取點名字（APN）、網際網路協定（IP）位址、輪詢時間（RTT）、可用輸送量、開放可用埠、回載資訊、行動性、信號強度、上傳/下載速率、頻寬等等）、訂閱資訊（例如，可用的用戶辨識/標識模組（SIM）卡、公共陸地行動網路（PLMN）、行動網路服務供應商（MNO）、追蹤區域等等）、位置資訊（例如，全球定位系統（GPS）可用性、位置座標等等）、系統資訊（例如，可用記憶體、中央處理單元（CPU）資訊、CPU使用、執行服務、啟用的螢幕/顯示器、可用的觸摸能力等等）、公知的易受攻擊性資訊（例如，諸如OS版本、OS已安裝補丁之類的作業系統（OS）資訊；諸如安全資料傳輸層（SSL）版本、SSL實現之類的安全資訊；諸如專家級AES之類的弱的或過期的安全演算法等等）和感測器資料（例如，感測器可用性、感測器資料等等）的一或多個的任意組合。

【0036】 在一些實施方式中，該蜜罐系統可以利用各種模組、部件、指令、操作、電路及/或常式來執行因果關係及/或行為分析操作、監聽及/或其他操作以偵測、控制及/或預測該行動計算設備內的活動。在一些實施方式中，該蜜罐系統可以經由蜜罐系統控制模組（例如，圖1

的蜜罐系統控制模組140）生效。例如，此蜜罐系統控制模組可以是OS服務、軟體、電路、模組、常式等等，其配置有對該行動計算設備中的系統級資源及/或信號傳遞的存取。在一些實施方式中，該蜜罐系統可以使用諸如高通公司的高通Snapdragon智慧防護之類的即時分析平臺辨識潛在的惡意應用程式。

【0037】 各個實施例提供使用行為分析和預測以觸發或誘發應用程式在受控制的行動環境中的隱藏惡意活動的動態蜜罐系統。具體來講，揭示的各種實現反覆運算地預測潛在惡意應用程式要求的觸發條件並且持續調整可用資源直到觀察到惡意活動為止。該等新穎技術適用於偵測未知惡意軟體或其他威脅的易攻擊性，因為各種實施方式不要求預定義的觸發條件而是分析應用程式行為和特性以便動態辨識測試中要使用的資源。該等技術亦可以降低監聽和偵測成本。

【0038】 各個實施例不同於監聽應用程式以辨識惡意軟體的現有技術。例如，一些現有技術簡單地提供已知惡意軟體可以預期的設備輸入（例如，虛擬按鍵），但是並不動態地改變行動計算設備操作條件或環境。該等現有技術不是預測性的並且不會至少部分地基於觀察到的應用程式的非惡意活動反覆運算地提供不同資源。各種實現可以使用行動計算設備的狀態資訊和系統資源資訊，以引起未辨識的或未知的惡意軟體的惡意活動，並且因此不依賴於使用明顯的致使已知惡意軟體啟用的輸入機制。

【0039】 與其他現有技術不同，各種實現不僅僅採用軟體或計算系統的靜態配置。例如，本案中揭示的各種實施方式並不反覆運算地實現針對不同作業系統或架構的預定義軟體安裝（或系統鏡像）的集合。相反，各種實施方式至少部分地基於對潛在惡意應用程式的行為分析（例如，當前許可、歷史活動）動態地改變個體資源（例如，可用硬體設備部件、系統狀態變數值等等）。該等動態改變並不基於已知的使用或已知造成惡意軟體活動的具體場景。例如，基於未知應用程式的當前行為，用各種實現配置的行動設備可以評估該等行為並且反覆運算地改變任意數量的可用設備部件、設備部件配置或操作狀態（例如，連線性）及/或系統條件（例如，電池功率位準等等）。

【0040】 一些現有技術監聽電腦系統中的具體內容的移動（例如，輸出傳輸中的資料）。各種實施方式不僅是浮水印或僅僅監聽具體資料或檔案是否已經移動了。相反，各種實施方式評估潛在惡意應用程式的各種活動，以預測促使惡意活動所需要的觸發條件。換言之，各種實施方式並不簡單地追蹤某些已經被洩漏出去的資料、提供浮水印或辨識到敏感性資料的存取路徑。

【0041】 圖1圖示根據各種實施方式的包括被配置為用作蜜罐系統的行動計算設備102的通訊系統100。行動計算設備102可以經由有線或無線連接103（例如，Wi-Fi網路連接、蜂巢網路連接等等）在一或多個網路105上交換通訊。例如，行動計算設備102可以與一或多

個遠端伺服器110交換資料，該等遠端伺服器亦經由有線或無線連接111連接到一或多個網路105。在各種實施方式中，網路105可以包括區域網路（LAN）及/或廣域網路（WAN），並且可以與各種存取點（諸如，Wi-Fi路由器、蜂巢網路基地台等等）相關聯。

【0042】 在各種實施方式中，行動計算設備102可以是各種類型的行動計算設備的任意一種，諸如平板電腦、智慧型電話和膝上型電腦。在一些實施方式中，一或多個遠端伺服器110可以包括各種第三方伺服器（例如，可以經由網際網路存取的網路伺服器、應用程式商店伺服器等）及/或與蜜罐系統監聽相關聯的伺服器計算設備（例如，管理關於惡意軟體應用程式的資料的安全伺服器等等）。

【0043】 在各種實施方式中，行動計算設備102可以包括一或多個處理器121。例如，行動計算設備102可以包括一或多個中央處理單元（CPU）（或應用程式處理器）、數位信號處理器（DSP）、圖形處理單元（GPU）或其任意組合。行動計算設備102亦可以包括能夠儲存處理器可執行指令（例如，應用程式、程式、常式、作業系統等等）、資料（例如，應用程式資料、訊息、簡檔、圖片、音訊檔案等）及/或其他用於執行如本案中所描述的各種操作的其他資訊的各種記憶體/資料儲存單元122（例如，RAM、緩存、硬體驅動器、快閃記憶體驅動器等等）。行動計算設備102的各種部件（例如，121-130）可以

經由有線及/或無線連接（諸如經由匯流排132）耦合到一起。

【0044】 行動計算設備102亦可以包括根據各種實施方式用於實現蜜罐系統所必須或不必須的可選部件。例如，行動計算設備102可以包括用於與其他設備及/或網路交換通訊的一或多個網路介面130。為了簡化的目的，該網路介面可以指的是，或者包括用於根據各種無線電存取技術、協定及/或格式來交換無線信號的任何硬體（例如，收發機、天線、連接器等等）及/或軟體（例如，邏輯、韌體等等）。例如，該網路介面可以包括Wi-Fi、藍芽®、RF及/或近場通訊（NFC）無線電單元。行動計算設備102可以包括一或多個感測器124（例如，攝像機、麥克風、光感測器、加速計、陀螺儀等等）。行動計算設備102亦可以包括各種輸入設備126，諸如觸控式螢幕輸入、周邊設備（例如，滑鼠、鍵盤等等）。行動計算設備102亦可以包括各種輸出設備128，諸如觸控式螢幕顯示器、燈泡、揚聲器等等。在一些實施方式中，行動計算設備102亦可以包括全球定位系統（GPS）接收器。

【0045】 各個可選部件可以被認為是可選的，因為在一些實施方式中行動計算設備102可以配置為簡單地模仿該等部件或相關功能，而無需要求實際的部件出現在行動計算設備102中。例如，行動計算設備102可以不包括實際的藍芽®無線電單元，但是可以為了使藍芽資源對於應

用程式可用以便觸發該處理器121上執行的應用程式的惡意活動的目的模仿藍芽®無線電單元的出現。

【0046】 在各種實施方式中，行動計算設備102可以被配置有能夠至少實現行動計算設備102(亦即，蜜罐系統)上的對惡意應用程式活動的監聽、分析和預測的各種軟體、服務、部件、模組、電路及/或其他功能。本質上，該蜜罐系統可以是對潛在惡意應用程式不可見的，但是能夠控制該潛在惡意應用程式與該行動設備102的各種系統部件、資料和能力的每次互動。在一些實施方式中，行動計算設備102的處理器121可以經由執行蜜罐系統控制模組140來使蜜罐系統生效。蜜罐系統控制模組140可以配置為繼續產生、截獲和過濾該系統內的信號，以控制可由潛在惡意應用程式使用的資訊和資源。例如，蜜罐系統控制模組140可以截獲或者偵測API呼叫以及任何設備級或OS級訊息傳輸，諸如從已安裝應用程式向輪詢感測器請求或者從記憶體或其他資料儲存單元接收儲存的資料。

【0047】 在一些實施方式中，蜜罐系統控制模組140可以包括及/或利用各種模組(例如，邏輯、軟體、電路等等)以提供該蜜罐系統。例如，蜜罐系統控制模組140可以利用配置為評估系統資訊(例如，狀態變數、存取等等)並執行機器學習以便辨識潛在惡意應用程式的出現的行為觀察和分析模組144。例如，行為觀察和分析模組144可以被配置為評估某個應用程式的應用程式許可、先

前執行的API呼叫及/或資源存取（例如，記憶體存取、網路連接查詢等等），以計算該應用程式是惡意軟體或者不是的概率。至少部分地基於此分析，該行為觀察和分析模組144可以將該應用程式辨識為潛在地具有惡意的或者不是。

【0048】 蜜罐系統控制模組140亦可以利用應用程式行為預測模組146，後者被配置為預測可以使該目標應用程式呈現惡意活動的觸發條件。例如，應用程式行為預測模組146可以執行目標應用程式、相關特性和先前觀察到的活動的輔助分析以辨識行動計算設備102的先前亦沒有可用但是若可用則會使惡意軟體啟用的一或多個資源或操作條件。

【0049】 蜜罐系統控制模組140可以利用動態資源選擇模組148，後者被配置為選擇可以使用及/或調整以便觸發潛在惡意應用程式的惡意活動的各種資源及/或系統狀態。對該等資源及/或系統狀態的選擇可以以設計為增加滿足辨識出的觸發條件的可能性的方式來完成。

【0050】 蜜罐系統控制模組140亦可以利用動態資源提供模組150，後者被配置為向潛在惡意應用程式提供所選擇的資源。例如，該動態資源提供模組150可以建立及/或調整虛擬的（或模仿的）資源（例如，虛擬網路連接或介面，諸如Wi-Fi網路連接、向具體MNO的註冊等等）。舉另一個實例，動態資源提供模組150可以配置實際資源可見但是僅具有對應用程式的有限存取的（例如，

使無法照相的攝像機感測器可見）。動態資源提供模組150可以使資源對應用程式的群組在系統範圍內可見或者僅對特定應用程式可見。

【0051】 蜜罐系統控制模組140亦可以利用蜜罐系統監聽模組152，後者被配置為監聽和觀察各種資源（例如，系統狀態資訊、設備狀態等等）以及潛在惡意應用程式的任何操作及/或狀態。例如，蜜罐系統監聽模組152可以被配置為截獲並評估來自特定目標應用程式的任何API呼叫、OS請求、中斷、信號及/或其他通訊。

【0052】 蜜罐系統控制模組140亦可以利用惡意活動偵測模組154，後者被配置為將新的觀察與先前觀察到的對應於潛在惡意應用程式的資訊組合起來以偵測惡意活動。例如，惡意活動偵測模組154可以偵測目標應用程式在若干行為分析的反覆運算上的動作趨勢並且決定動作組合可能表示惡意活動。

【0053】 圖2-圖5是根據各種實施方式圖示可以由被配置為用作蜜罐系統的行動計算設備102使用的動態資料200的實例的示意圖。動態資料200可以對應於行動計算設備102在根據本案中描述的各種實施方式用於決定潛在惡意應用程式的觸發條件的反覆運算行為分析演算法的執行期間儲存的資訊。在一些實施方式中，動態資料200和反覆運算行為分析演算法可以如前述由蜜罐系統控制模組140更新、管理、執行或者控制。

【0054】 出於非限制性解釋說明的目的，圖2-圖5處理行動計算設備102已辨識出目標應用程式250（或者目標「應用程式」）為潛在惡意應用程式的場景。此辨識可以至少部分地基於如前述的經由行為觀察和分析模組144對目標應用程式250的許可及/或先前活動的分析。動態資料200可以對應於行動計算設備102在關於目標應用程式250的反覆運算行為分析演算法的執行期間儲存的資訊。動態資料200可以包括：指示在給定的時間提供的或者「可見的」以便由目標應用程式250使用的當前資源（例如，設備部件、系統狀態的資料）的資源資料分段202a-202d；指示對目標應用程式250的許可的許可資料分段204；及指示當前目標應用程式250活動（例如作為對資源及/或狀態資訊的調整的回應的API呼叫等等）的活動資料分段206a-206d。出於在圖2-圖5中圖示的實例的目的，許可資料分段204可以指示目標應用程式250具有對存取各種網路功能（例如，蜂巢網路連接、Wi-Fi網路連接等等），以及記憶體及/或儲存設備存取（例如，向記憶體、硬碟、外部儲存讀取/寫入資料等）的許可。

【0055】 在各種實施方式中，行動計算設備102可以使用用於儲存、定義、顯示（或使其可存取）和追蹤與目標應用程式250及/或行為分析演算法相關聯的資料的各種資料結構和記錄方案。圖2-圖5中圖示的任何資料或資料結構僅僅是示例性的，而非限制資料管理的其他方式。

【0056】 圖2圖示在行為分析演算法的第一次反覆運算之後由行動計算設備102儲存的動態資料200。具體來講，動態資料200可以包括資源資料分段202a，資源資料分段202a包括指示蜂巢網路介面存在於行動計算設備102中的資料。動態資料200亦可以包括活動資料分段206a，活動資料分段206a指示目標應用程式250亦沒有執行任何動作或者另外亦沒有執行與該可用蜂巢網路連接的任何潛在惡意動作。具體來講，目標應用程式250可能僅執行了對當前網路連接的檢查，此舉可以是執行在行動計算設備上的很多良性應用程式的常見操作。

【0057】 由於在該行為分析演算法的第一次反覆運算之後沒有偵測到惡意活動，行動計算設備102可以使用動態資料200中的資料的任意組合以執行該行為分析演算法的第二次反覆運算，以便預測目標應用程式250的觸發條件。具體來講，行動計算設備102可以評估對目標應用程式250的許可（例如，網路和儲存/記憶體存取）與目標應用程式250的可用的當前資源（例如，蜂巢網路）的組合，以便預測目標應用程式250可以在執行惡意動作之前等待的條件及/或資源。可以如前述使用應用程式行為預測模組146做出該等預測。

【0058】 例如，經由該行為分析演算法，行動計算設備102可以觀察目標應用程式250具有網路存取許可，具有對敏感性資料的存取並且僅執行與蜂巢網路連接的良性活動（例如，檢查可用網路連接（例如，RAT可用性、

對特定非共用位址的網域名稱系統（DNS）查詢等等））。作為對此觀察的回應，行動計算設備102可以推斷目標應用程式250具有很高概率使用WAN連接來洩露敏感資訊。行動計算設備102亦可以預測目標應用程式250尋找不同類型的網路連接或RAT（例如，Wi-Fi），以用於洩漏敏感資訊。

【0059】 至少部分地基於該等預測，行動計算設備102可以提供僅對目標應用程式250可見的虛擬Wi-Fi網路連接或介面，諸如經由如前述的動態資源選擇模組148和動態資源提供模組150。虛擬Wi-Fi網路連接可以被緊密地監聽並且具有受限的網路連接。行動計算設備102能夠偵測經由新的Wi-Fi網路連接發送的（或請求要發送的）任何通訊，諸如經由如前述的蜜罐系統監聽模組152。

【0060】 圖3圖示在此實例的行為分析演算法的第二次反覆運算和提供虛擬Wi-Fi網路連接之後由行動計算設備102儲存的動態資料200。該資源資料分段202b指示行動計算設備102提供Wi-Fi網路連接以取代如圖2中所示的蜂巢網路連接。作為對改變目標應用程式250可用的網路連接類型的回應，動態資料200現在可以包括活動資料分段206b，活動資料分段206b指示目標應用程式250執行操作以存取敏感性資料（例如，密碼檔案、連絡人清單等等），並且隨後經由虛擬Wi-Fi網路連接操作外部資料轉移。行動計算設備102可以決定目標應用程式250的該等動作是潛在地具有惡意的，諸如經由如前述的

惡意活動偵測模組154。使用此反覆運算的行為分析演算法，行動計算設備102可能已經至少決定目標應用程式250可能被設計為僅使用Wi-Fi網路連接（例如，不使用蜂巢網路）來進行盜取/散發敏感性資料的惡意活動。

【0061】 在一些情況中，行動計算設備102可以執行行為分析演算法的額外反覆運算以觸發目標應用程式250的惡意活動。例如，若目標應用程式250被配置為僅在滿足若干條件時執行惡意活動，則行動計算設備102可以重複地執行分析、預測和提供操作直到出現引起惡意活動的準確的因素組合為止。

【0062】 圖4圖示回應於從蜂巢網路連接到Wi-Fi網連接的改變，目標應用程式250不開始執行惡意動作的示例性場景。具體來講，圖4圖示在行為分析演算法的第二次反覆運算和提供資源資料分段202c所指示的虛擬Wi-Fi網路連接之後儲存的動態資料200。在此實例中，活動資料分段206c不指示回應於新提供的Wi-Fi網路連接目標應用程式250執行了潛在的惡意動作。

【0063】 由於正在該行為分析演算法的第二次反覆運算之後沒有偵測到惡意活動，行動計算設備102可以使用動態資料200中的資料的任意組合來執行該行為分析演算法的第三次反覆運算，以預測目標應用程式250的觸發條件。行動計算設備102可以評估目標應用程式250的許可（例如，網路和儲存/記憶體存取）與目標應用程式250可用的當前資源（例如，Wi-Fi網路連接）的組合。隨後，

行動計算設備102可以預測目標應用程式250在執行惡意動作之前可以等待的條件及/或資源。

【0064】 例如，經由行為分析演算法，行動計算設備102可以觀察目標應用程式250具有不同類型的網路存取加上對某些敏感性資料的存取，但是僅執行了良性的活動。作為回應，行動計算設備102可以推斷目標應用程式250可能有很高概率盜取行動計算設備102可以存取敏感性資料但是不會本機儲存任何資料的資訊。在此種環境中，行動計算設備102可以預測目標應用程式250可以等待包含該目標應用程式250被設計盜取的特定類型資料的新的資料來源。至少部分地基於該預測，行動計算設備102可以建立到假的外部資料來源（或驅動）的虛擬連接，諸如經由無線或有線連接（例如，藍芽®、NFC、電纜等等）連接的硬驅動或者經由通用序列匯流排（USB）連接來連接的優盤等等。行動計算設備102能夠偵測向該新的假的外部資料來源的任何資料存取（例如，複製、寫入、讀取等等）。

【0065】 圖5圖示在該行為分析演算法的第三次反覆運算和提供到該假的外部資料來源的連接之後由行動計算設備102儲存的動態資料200。資源資料分段202d指示行動計算設備102除了先前提供的Wi-Fi網路連接之外亦提供到外部資料來源（或驅動）的連接。作為對所提供資源的改變的回應，動態資料200現在包括活動資料分段206d，活動資料分段206d指示目標應用程式250開始

操作以存取外部驅動（例如，複製資料等等），隨後操作在該Wi-Fi網路連接上的外部資料轉移；可能是具有惡意的活動。換言之，使用反覆運算行為分析演算法，行動計算設備102在此實例中決定目標應用程式250被設計為至少使用Wi-Fi網路連接以進行從行動計算設備102外部的資料來源盜取和散發資料的惡意活動。

【0066】 圖6圖示根據各種實施方式用於行動計算設備使用行為分析和動態資源提供來觸發應用程式的惡意活動的方法600。在一些實施方式中，方法600的各種操作可以由蜜罐系統控制模組140和各種模組（例如，模組144-154）來執行，每個經由該行動計算設備的處理器（例如，行動計算設備102的處理器121）來執行。

【0067】 在方塊602中，行動計算設備的處理器可以分析安裝在該行動計算設備的儲存上及/或執行在該行動計算設備的處理器上的一或多個應用程式以估計該等應用程式可能具有惡意的概率。例如，該行動計算設備可以評估執行在該處理器上的每個應用程式的許可，以辨識該行動計算設備的可以由該應用程式存取的潛在子系統及/或其他功能。該行動計算設備可以至少部分地基於先前觀察到的並且儲存的每個應用程式的資料（例如，該等應用程式的歷史活動、當前許可等等）來計算該一或多個應用程式中的每一個潛在地具有惡意的概率。在一些實施方式中，某些許可、先前的動作或其任意組合可以指示一個應用程式具有更高概率是惡意軟體。例如，該行動計算設備

可以由於一個應用程式存取該行動計算設備的特定部件（例如，網路介面）及/或敏感性資料的能力而計算該應用程式有很高概率能夠執行惡意資料洩漏操作。舉另一個實例，該行動計算設備可以基於將惡意應用程式的已知行為與在該行動計算設備上執行期間觀察到的該應用程式的當前（或最近）行為匹配，而計算該應用程式有很高概率能夠執行惡意資料洩漏操作。

【0068】 在判定方塊604中，該行動計算設備的處理器可以決定當前安裝在該行動計算設備的儲存上及/或在該行動計算設備的處理器上執行的一或多個應用程式的任何一個是否是潛在地具有惡意的。例如，該行動計算設備可以將計算出的該應用程式具有惡意的概率與閾值比較，以決定一個應用程式是否應該被歸類為潛在地具有惡意的。在一些實施方式中，方塊602-604的操作可以使用如上參考圖1描述的行為觀察和分析模組144來執行。

【0069】 作為對決定當前在該行動計算設備的處理器上執行的一或多個應用程式中沒有一個潛在地具有惡意（亦即，判定方塊604=「否」）的回應，該行動計算設備可以繼續進行方塊602中的分析操作，或者若所有應用程式皆已經被分析並發現很可能是良性的則結束。

【0070】 作為對決定該行動計算設備的處理器上當前執行的一或多個應用程式潛在地具有惡意（亦即，判定方塊604=「是」）的回應，該行動計算設備的處理器可以在方塊606中選擇潛在地具有惡意的目標應用程式。例

如，所選擇的目標應用程式可以簡單地是複數個辨識出的潛在惡意應用程式中的下一個。在一些實施方式中，該行動計算設備可以選擇複數個（或組合）目標應用程式以評估方塊606-622的操作。換言之，由該行動計算設備進行的方塊606的選擇可以不僅限於一個目標應用程式，而是該蜜罐系統可以針對可能具有相似（或者相同）觸發參數的一組應用程式來執行。

【0071】 在方塊608中，該行動計算設備的處理器可以預測可以激起或觸發該目標應用程式（或目標應用程式的組合）的惡意活動的觸發條件（例如，可用資源、系統狀態等等）。例如，該行動計算設備可以預測該目標應用程式要求Wi-Fi網路連接以開始惡意動作，即使Wi-Fi網路連接實際上並不可用。在一些實施方式中，該行動計算設備可以經由評估對目標應用程式（或目標應用程式的組合）的許可、先前對於該目標應用程式可存取的任何資源和儲存的指示該目標應用程式的先前活動的活動資料，做出對觸發條件的該等預測，以便辨識該目標應用程式可以在開始惡意行為之前等待的狀況。在一些實施方式中，方塊608的操作可以使用如上參考圖1所描述的應用程式行為預測模組146執行。例如，該行動計算設備可以基於在該目標應用程式執行中直到當前時間觀察到的相關動作，做出關於未來可能由該目標應用程式存取的動作或資源（例如，藍芽通訊）的預測，諸如針對該行動計算設備的藍芽部件的出現或狀態的查詢。

【0072】 在方塊610中，該行動計算設備的處理器可以辨識要提供的可以滿足該預測出的觸發條件的資源（例如，設備部件、系統狀態資料）。例如，至少部分地基於預測出的指示該目標應用程式要求Wi-Fi網路連接以開始惡意動作的觸發條件，該行動計算設備可以辨識應該模仿假的Wi-Fi網路介面或者使其對該目標應用程式可見。在一些情況中，該行動計算設備可以辨識已經可用的資源應該被調整或重新配置以滿足該預測的觸發條件。例如，信號強度讀取可能需要被人為地增加或減少。在一些實施方式中，該行動計算設備可以迫使可用資源進入例外條件以便向該目標應用程式（或目標應用程式的組合）顯示可能觸發額外的惡意行為的極端案例。

【0073】 如前述，可以被辨識為用於提供的資源可以包括設備部件和資料中的一或多個（例如，系統變數、OS級別資料、暫存器資料等等）。例如，設備部件可以包括已安裝的應用程式、作業系統、網路介面、處理單元、資料儲存單元、耦合的設備、輸出單元、輸入單元和感測器。舉另一個實例，資源資料可以包括連絡人清單、儲存的檔案、個人資訊、網路狀況資料、訂閱資訊、位置資訊、系統資訊、已知易受攻擊資訊和感測器資料。

【0074】 為了觸發特定的複雜惡意應用程式，動態提供資源及/或對資源的調整應該儘可能實際地呈現給目標應用程式（或目標應用程式的組合）。例如，該目標應用程式應該不能從實際存在於該行動計算設備的網路中的真

實網路條件來區分出假的或模仿的網路條件。舉另一個實例，現實的電話連絡人清單可以包括具有多於一個區域碼的電話號碼。舉另一個實例，訊息日誌可以指示該行動計算設備已經與該連絡人清單中的一些而不是全部連絡人交換過多個簡訊服務（SMS）訊息。此外，動態資源應該以與實際資源一致的隨機性水平來出現、改變和消失。例如，由於Wi-Fi網路連接無法在典型Wi-Fi傳輸範圍之外維持，因此單個Wi-Fi存取點在其他資料指示該行動計算設備遠超過典型Wi-Fi存取點可達到範圍時不應該被報告為活動的。

【0075】 因此，在方塊610中，該行動計算設備可以辨識與預測的該目標應用程式（或目標應用程式的組合）的觸發條件直接及/或間接相關的資源。例如，為了避免惡意軟體應用程式偵測到蜜罐系統環境的出現，該行動計算設備可以呈現或模擬移動資訊（例如，感測器或改變GPS資料）和不同連接的存取點的提供（例如，SSID、媒體存取控制（MAC）位址、RSSI）二者。舉另一個實例，為了提供更真實的可由該目標應用程式存取的假的連絡人清單，該行動計算設備可以決定更多不同連絡人需要被添加到該假的連絡人清單中（例如，來自不同區域碼的電話號碼、各種數量的SMS訊息的不同接收方/發送方等等）。在一些實施方式中，方塊610的操作可以使用如上參考圖1所描述的動態資源選擇模組148來執行。

【0076】 在方塊612中，該行動計算設備的處理器可以提供辨識出的資源。在一些情況中，提供可以包括至少部分地基於預測的觸發條件調整已經可用的（或可見的）資源，諸如經由改變設備部件的操作特性（例如，輸送量、處理速度、溫度讀數等等）及/或調整可以由該目標應用程式輪詢的系統資料的值。例如，該行動計算設備可以調整該目標應用程式可請求以指示特定信號強度、存取點名稱、存取網路等等的網路連接狀態資料。舉另一個實例，該行動計算設備可以改變GPS資料以指示該行動計算設備已經重新定位到新的城市。提供亦可以包括配置對該目標應用程式（或目標應用程式的組合）可見的資源，即使在該等資源通常不存在於該行動計算設備上時。例如，該行動計算設備可以啟用特定網路介面及/或感測器，用於由該目標應用程式的潛在使用。舉另一個實例，該行動計算設備可以至少部分地基於預測出的觸發條件來調整先前對目標應用程式可見的資源（例如，調整操作參數或配置）。舉另一個實例，該行動計算設備可以配置先前對目標應用程式不可見的資源，使該資源變得對該目標應用程式可見或者可存取。

【0077】 在一些實施方式中，提供可以包括至少部分地基於預測出的觸發條件建立虛擬資源。該等虛擬資源可以代表沒有實際出現在該行動計算設備中或者由其支援的模仿的設備部件及/或資料。例如，該行動計算設備可以產生對於該目標應用程式可見並且可存取的虛擬（或假

的）Wi-Fi網路介面、假的藍芽®無線電單元、假的SIM卡、耦合的外部設備（例如，USB優盤等等）及/或假的DSP。在一些實施方式中，方塊612的操作可以使用如上參考圖1描述的動態資源提供模組150執行。

【0078】 在方塊614中，行動計算設備的處理器可以監聽該目標應用程式（或目標應用程式的組合）對應於新提供的資源的活動（例如，對所提供的資源的存取）。例如，該行動計算設備可以截獲及/或偵測所有應用程式介面（API）呼叫、中斷、訊息及/或該目標應用程式發出的其他信號傳遞。所監聽的活動可以包括諸如請求OS級別服務、對記憶體或其他儲存的讀取/寫入、使用更多功率及/或處理器時間、對系統變數或資料的查詢或改變、經由網路介面發起通訊、輪詢設備部件（例如，感測器）及/或使用該行動計算設備的一或多個資源執行任何其他操作之類的動作。

【0079】 在方塊616中，該行動計算設備的處理器可以至少部分地基於方塊614的監聽操作更新針對目標應用程式（或目標應用程式的組合）儲存的活動資料。在一些實施方式中，該行動計算設備可以將所有評估的應用程式的歷史和狀態維護一段時間。該等歷史活動資料可以被保存在與個體目標應用程式相關聯的各種資料結構中，諸如應用程式簡檔。例如，該行動計算設備可以更新與該目標應用程式相關聯的簡檔資料以指示任何API呼叫、記憶體存取及/或由該目標應用程式發起的其他動作，作為對各

種提供操作的回應。在一些實施方式中，該行動計算設備可以將歷史活動資料儲存在與目標應用程式的組合相關聯的各種資料結構或簡檔中。在一些實施方式中，方塊614-616的操作可以使用如上參考圖1所描述的蜜罐系統監聽模組152執行。

【0080】 在判定方塊618中，該行動計算設備的處理器可以決定該目標應用程式（或目標應用程式的組合）是否進行任何惡意活動。此判定可以包括對作為對使資源可用或調整資源的回應出現的監聽到的該目標應用程式的活動進行評估。例如，作為對產生可用於由該目標應用程式存取的假的連絡人清單的回應，該行動計算設備可以在當該連絡人清單被傳遞以經由該目標應用程式可存取的出站連接（例如，Wi-Fi連接、蜂巢網路連接等等）傳輸時決定發生惡意活動。在一些實施方式中，此決定亦可以包括評估儲存的指示該目標應用程式的先前活動的活動資料。例如，當該目標應用程式先前複製了敏感性資料並且重複地檢查可用Wi-Fi連接但是沒有嘗試傳輸該複製的資料時，該行動計算設備可以在該目標應用程式稍後被觀察到請求與遠端資料來源建立連接時，決定在發生惡意活動。在各種實施方式中，該行動計算設備可以至少部分地基於觀察到的活動資料（例如，截獲的API呼叫、中斷及/或由該目標應用程式產生或者發起的其他信號）辨識惡意活動，該觀察到的活動資料被轉發給分析器作為對方塊612的提供操作的回應。在一些實施方式中，判定方塊

618的操作可以使用如上參考圖1所描述的惡意活動偵測模組154執行。

【0081】 作為對決定沒有偵測到對應於該目標應用程式的惡意活動（亦即，判定方塊618=「否」）的回應，該行動計算設備可以繼續進行方塊608中的預測操作。換言之，該行動計算設備可以反覆運算地決定如何提供資源和相應地重新提供資源直到該目標應用程式回應為止。例如，至少部分地基於新觀察到的該目標應用程式的行為，該行動計算設備可以更新行為預測並且辨識要模仿的或者要調整的新的資源以觸發該目標應用程式。不同資源及/或系統狀態資料可以替代及/或添加到先前可用的資源及/或提供給該目標應用程式的系統狀態資料。

【0082】 在一些實施方式中，該行動計算設備可以使用蜜罐系統觀察，以更新方塊602中由該目標應用程式進行惡意活動的概率，並且因此可以決定該目標應用程式可能不具有惡意。例如，在方塊608-618的操作的若干次反覆運算之後，該行動計算設備可以決定該目標應用程式是惡意軟體的概率低於閾值，並且將該目標應用程式從潛在惡意應用程式清單中移除。當此種情況發生時，該行動計算設備可以在方塊606中選擇下一個目標應用程式並且繼續進行聚焦在該目標應用程式上的方法600的操作。

【0083】 作為對決定在目標應用程式中偵測到惡意活動（亦即，判定方塊618=「是」）的回應，該行動計算設備的處理器可以決定所預測出的觸發條件是準確的，或

者記錄當前提供的資源，並且在方塊620中將關於當前提供的資源的資訊儲存為滿足該目標應用程式(或目標應用程式的組合）的觸發條件。

【0084】 在一些實施方式中，該行動計算設備可以執行各種操作，作為對偵測到該目標應用程式(或目標應用程式的組合）的惡意活動的回應。例如，基於偵測到的惡意行為，該行動計算設備可以阻止目標應用程式存取某些資源及/或停用該目標應用程式。作為對偵測惡意活動的回應執行的操作的另一個非限制性實例，該行動計算設備可以執行報告操作。因此，在可選方塊622中，該行動計算設備的處理器可以傳輸指示該目標應用程式(或目標應用程式的組合）的觸發條件的報告訊息。例如該行動計算設備可以與伺服器通訊，該伺服器被配置為登記關於在該行動計算設備上提供的促使該目標應用程式呈現惡意行為的部署的資源的惡意軟體資料以及觀察的惡意行為的類型(例如，洩漏敏感性資料的應用程式）。舉另一個實例，該行動計算設備可以警告其他行動計算設備(例如，在該行動計算設備附近的或者經由通訊媒體可到達的設備等等）關於部署的資源和相應惡意行為。該等其他設備可以選擇針對類似的該等設置監聽各自的本端應用程式。

【0085】 在判定方塊624中，該行動計算設備的處理器可以決定是否存在要監聽的任何其他潛在惡意應用程式。作為對決定存在要監聽的其他潛在惡意應用程式(亦即，判定方塊624=「是」）的回應，該行動計算設備可

以在方塊606中選擇另一個目標應用程式來監聽並且聚焦在該應用程式上繼續進行方法600的操作。作為對決定沒有其他潛在惡意應用程式要監聽(亦即，判定方塊624=「否」）的回應，該行動計算設備可以結束方法600。

【0086】 各種形式的行動計算設備，包括個人電腦和膝上型電腦，可以用於實現各種實現。該等計算設備典型地包括圖7中圖示的部件，其圖示示例性智慧型電話行動計算設備700。

【0087】 在各種實施方式中，該行動計算設備700可以包括耦合到觸控式螢幕控制器704和內部記憶體702的處理器701。該處理器701可以是針對一般或專用處理任務指定的一或多個多核IC。內部記憶體702可以是揮發性及/或非揮發性記憶體，並且亦可以是安全的及/或加密的記憶體，或者不安全的及/或未加密的記憶體，或者其任意組合。該觸控式螢幕控制器704和處理器701亦可以耦合到觸控式螢幕面板712，諸如電阻感測觸控式螢幕、電容感測觸控式螢幕、紅外感測觸控式螢幕等等。

【0088】 行動計算設備700可以具有相互耦合及/或耦合到該處理器701的一或多個無線電信號收發機708（例如，藍芽、ZigBee®、Wi-Fi、射頻（RF）收發機）和天線710，用於發送和接收。收發機708和天線710可以與上述電路一起使用以便實現各種無線傳輸協定堆疊和介面。該行動計算設備700可以包括能夠經由蜂巢網路通訊並且耦合到該處理器的蜂巢網路無線數據機晶片716。

【0089】 該行動計算設備700可以包括耦合到該處理器701的周邊設備連接介面718。該周邊設備連接介面718可以唯一地配置為接受一個類型的連接，或者多重地配置為接受各種類型的共用的或私有的實體和通訊連接，諸如USB、火線介面、閃電介面或PCIe。該周邊設備連接介面718亦可以耦合到類似配置的周邊設備連接埠（未圖示）。

【0090】 該行動計算設備700亦可以包括用於提供音訊輸出的揚聲器714。該行動計算設備700亦可以包括由塑膠、金屬或合成材料構造的外殼720，用於容納本案中論述的所有或一些部件。該行動計算設備700可以包括耦合到處理器701的電源722，諸如一次性的或可充電的電池。可充電電池亦可以耦合到周邊設備連接埠以便從該行動計算設備700外部的電源接收充電電流。

【0091】 圖示和描述的各個實現僅僅是作為實例提供的，以便解釋說明請求項的各個特徵。但是，關於任何給定實現圖示並描述的特徵並不必須僅限於相關聯的實現，而是可以圖示和描述的其他實現一起使用或組合起來。此外，請求項並不意在受到任何一個示例性實現的限制。

【0092】 本案中描述的各種處理器可以是能夠由軟體指令（應用程式）配置為執行各種功能（包括本案中描述的各個實現的功能）的任何可程式設計微處理器、微電腦或多處理器晶片或晶片組。在各個設備中，可以提供多個

處理器，諸如專用於無線通訊功能的一個處理器和專用於執行其他應用程式的一個處理器。通常，軟體應用程式可以在其被存取並載入到處理器中之前儲存在內部記憶體中。該等處理器可以包括足夠儲存該等應用程式軟體指令的內部記憶體。在很多設備中，該內部記憶體可以是揮發性的或非揮發性的記憶體，諸如快閃記憶體或其混合。為了此說明書的目的，對記憶體的一般引用指的是可由處理器存取的記憶體，包括內部記憶體或插入到各種設備的可移除記憶體和處理器內部的記憶體。

【0093】 上述方法描述和程序流程圖僅僅作為示例性實例提供，而並不意在要求或暗示各個實現的操作必須以圖示的次序執行。熟習此項技術者應該瞭解的是，上述實現中的操作順序可以用任何次序執行。諸如像「之後」、「隨後」、「接下來」等術語並不意在限制操作的次序；該等術語僅僅用於貫穿方法描述引導讀者。此外，任何以單數形式對聲明元素的引用，例如使用冠詞「a」、「an」或「the」並不能解釋為將該元素限制為單數。

【0094】 結合本案中揭示的實現所描述的各種示例性的邏輯區塊、模組、電路和演算法操作可以實現成電子硬體、電腦軟體或其組合。為了清楚地說明硬體和軟體之間的可交換性，上文對各種示例性的部件、方塊、模組、電路和操作已經圍繞其各自功能進行了整體描述。至於此種功能是實現成硬體還是實現成軟體，取決於特定的應用和對整體系統所施加的設計約束條件。熟習此項技術者可以

針對每個特定應用，以變通的方式實現所描述的功能，但是，此種實現決策不應解釋為背離本發明請求項的保護範疇。

【0095】 用於執行本案所述功能的通用處理器、數位信號處理器（DSP）、特殊應用程式積體電路（ASIC）、現場可程式設計閘陣列（FPGA）或其他可程式設計邏輯設備、個別閘門或者電晶體邏輯設備、個別硬體部件或者其任意組合，可以實現或執行用於實現結合本案揭示實現描述的各種示例性的邏輯、邏輯區塊圖、模組和電路的硬體。通用處理器可以是微處理器，或者，該處理器亦可以是任何處理器、控制器、微控制器或者狀態機。處理器亦可以實現為計算設備的組合，例如，DSP和微處理器的組合、複數個微處理器、一或多個微處理器與DSP核心的結合，或者任何其他此種結構。另外，一些操作或方法可以由專用於給定功能的電路執行。

【0096】 在包括方法600的各種實現中，所描述的功能可以用硬體、軟體、韌體，或其任意結合來實現。若在軟體中實現，功能可以作為一或多個指令或代碼儲存在非暫時性處理器可讀取、電腦可讀取或伺服器可讀取媒體或非暫時性處理器可讀取儲存媒體上或經由其傳輸。本案中揭示的方法或演算法的操作可以實現在處理器可執行軟體模組或處理器可執行軟體指令中，該等指令可以常駐在非暫時性電腦可讀取儲存媒體、非暫時性伺服器可讀取儲存媒體及/或非暫時性處理器可讀取儲存媒體上。在各個實

現中，該等指令可以是儲存的處理可執行指令或儲存的處理器可執行軟體指令。有形的、非暫時性電腦可讀取儲存媒體可以是電腦可存取的任何可用媒體。舉個實例，但是並不作為限制，此種非暫時性電腦可讀取媒體可以包括RAM、ROM、EEPROM、CD-ROM或其他光碟儲存設備、磁碟儲存設備或其他磁儲存設備，或可以用於以指令或資料結構的形式儲存期望的程式碼並可以由電腦存取的任何其他媒體。本案中所用的磁碟和光碟，包括壓縮光碟（CD）、雷射光碟、光碟、數位多功能光碟（DVD）、軟碟和藍光光碟®，其中磁碟通常磁性地複製資料，而光碟則用鐳射光學地複製資料。上述的結合亦應該包含在非暫時性電腦可讀取媒體的範疇內。另外，方法或演算法的操作可以作為非暫時性處理器可讀取媒體及/或有形的非暫時性處理器可讀取儲存媒體及/或電腦可讀取媒體上的代碼及/或指令的一個或任何組合或集合，其可以整合到電腦程式產品中。

【0097】 提供前面對揭示實現的描述以便使任何熟習此項技術者能夠製作或使用本請求項的技術。對該等技術的修改對於熟習此項技術者來說是顯而易見的，並且本案中定義的一般原則可以在不脫離本發明的精神或範疇的前提下應用於其他實現。因此，本案內容並不意在限制本案中圖示的實現，而是與下文的請求項和本案中揭示的原則和新穎性特徵保持最廣泛範疇的一致。

【符號說明】

【0098】

100 通訊系統

102 行動計算設備

103 有線或無線連接

105 網路

110 遠端伺服器

111 有線或無線連接

121 處理器

122 記憶體/資料儲存單元

124 感測器

126 輸入設備

128 輸出設備

130 網路介面

132 匯流排

140 蜜罐系統控制模組

144 行為觀察和分析模組

146 應用程式行為預測模組

148 動態資源選擇模組

150 動態資源提供模組

152 蜜罐系統監聽模組

154 惡意活動偵測模組

200 動態資料

202a 資源資料分段

202b 資源資料分段

202c 資源資料分段

202d 資源資料分段

204 許可資料分段

206a 活動資料分段

206b 活動資料分段

206c 活動資料分段

206d 活動資料分段

250 目標應用程式

600 方法

602 方塊

604 判定方塊

606 方塊

608 方塊

610 方塊

612 方塊

614 方塊

616 方塊

618 判定方塊

620 方塊

622 可選方塊

624 判定方塊

700 行動計算設備

701 處理器

702 內部記憶體

704 觸控式螢幕控制器

708 無線電信號收發機

710 天線

712 觸控式螢幕面板

714 揚聲器

716 蜂巢網路無線數據機晶片

718 周邊設備連接介面

720 外殼

722 電源

【生物材料寄存】

【0099】 國內寄存資訊(請依寄存機構、日期、號碼順序註記)

無

【0100】 國外寄存資訊(請依寄存國家、機構、日期、號碼順序註記)

無

【序列表】(請換頁單獨記載)

無

【發明申請專利範圍】

【第1項】 一種實現在一蜜罐系統中用於觸發由應用程式進行的惡意活動的方法，包括以下步驟：

回應於決定一目標應用程式潛在地具有惡意，經由一計算設備的一處理器來預測該目標應用程式的一觸發條件；

至少部分地基於所預測的該觸發條件，經由該處理器來提供一或多個資源；

經由該處理器來監聽與所提供的該一或多個資源相對應的該目標應用程式的活動；及

至少部分地基於所監聽到的該等活動，經由該處理器來決定該目標應用程式是否是一惡意應用程式。

【第2項】 如請求項1之方法，其中經由該處理器監聽該目標應用程式的活動之步驟包括以下步驟：監聽可能具有相同觸發條件的一組應用程式。

【第3項】 如請求項1之方法，亦包括以下步驟：

經由該處理器來決定當前執行在該計算設備上的一應用程式是否是潛在地具有惡意的；及

回應於決定該應用程式潛在地具有惡意，指定該應用程式為該目標應用程式。

【第4項】 如請求項3之方法，其中經由該處理器來決定當前在該計算設備上執行的該應用程式是否是潛在

地具有惡意的之步驟包括以下步驟：

經由該處理器，分析以下各項中的至少一項：對與存取該計算設備的資源相對應的該應用程式的一許可，以及儲存的指示該應用程式的先前活動的活動資料。

【第5項】 如請求項 1 之方法，其中該一或多個資源包括一或多個設備部件和資料中的一項或兩項。

【第6項】 如請求項 5 之方法，其中該一或多個設備部件包括由一已安裝應用程式、一作業系統、一網路介面、一處理單元、一資料儲存單元、一耦合的設備、一輸出單元、一輸入單元和一感測器組成的該群組中的至少一個成員。

【第7項】 如請求項 5 之方法，其中該資料包括由一連絡人清單、一儲存的檔案、個人資訊、網路狀況資料、訂閱資訊、位置資訊、系統資訊、已知易損性資訊和感測器資料組成的該群組中的至少一個成員。

【第8項】 如請求項 1 之方法，其中回應於決定該目標應用程式潛在地具有惡意，經由該處理器來預測該目標應用程式的該觸發條件之步驟包括以下步驟：

經由該處理器，評估以下各項中的至少一項：對該目標應用程式的一許可、先前對於該目標應用程式可存取的任何資源和儲存的指示該目標應用程式的先前活動的活動資料。

【第9項】 如請求項1之方法，其中至少部分地基於所預測的該觸發條件經由該處理器來提供該一或多個資源之步驟包括以下各項步驟中的至少一項步驟：

至少部分地基於所預測的該觸發條件，經由該處理器來調整先前對於該目標應用程式可見的一資源；及

經由該處理器來配置先前對於該目標應用程式不可見的一資源，從而使該資源變得對於該目標應用程式可見。

【第10項】 如請求項1之方法，其中至少部分地基於所預測的該觸發條件經由該處理器來提供該一或多個資源之步驟包括以下步驟：

至少部分地基於所預測的該觸發條件，經由該處理器來建立一虛擬資源，其中該虛擬資源代表並非實際存在於該計算設備中或由該計算設備支援的模仿的一設備部件或資料。

【第11項】 如請求項1之方法，其中經由該處理器來監聽與所提供的該一或多個資源相對應的該目標應用程式的活動之步驟包括以下步驟：

經由該處理器來偵測由該目標應用程式進行的一應用程式介面（API）呼叫。

【第12項】 如請求項1之方法，其中至少部分地基於所監聽到的該等活動經由該處理器來決定該目標應用

程式是否是一惡意應用程式之步驟包括以下步驟：

經由該處理器來評估所監聽到的該等活動和儲存的指示該目標應用程式的先前活動的活動資料。

【第13項】 如請求項1之方法，亦包括以下步驟：經由該處理器來更新儲存的該目標應用程式的活動資料，該活動資料包括關於回應於決定該目標應用程式是一惡意應用程式而提供的資源的資訊。

【第14項】 如請求項1之方法，亦包括以下步驟：回應於決定該目標應用程式是一惡意應用程式，來傳輸指示該目標應用程式的該觸發條件的一報告訊息。

【第15項】 一種計算設備，包括：

一記憶體；及

一處理器，其被耦合到該記憶體並且被配置有處理器可執行指令，以執行包括以下各項的操作：

回應於決定一目標應用程式潛在地具有惡意，預測該目標應用程式的一觸發條件；

至少部分地基於所預測的該觸發條件，提供一或多個資源；

監聽與所提供的該一或多個資源相對應的該目標應用程式的活動；及

至少部分地基於所監聽到的該等活動，決定該目標應用程式是否是具有惡意的。

【第16項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而監聽該目標應用程式的活動包括：監聽可能具有相同觸發條件的一組應用程式。

【第17項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行亦包括以下各項的操作：

決定當前執行在該計算設備上的一應用程式是否是潛在地具有惡意的；及

回應於決定該應用程式潛在地具有惡意，指定該應用程式為該目標應用程式。

【第18項】 如請求項17之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而決定當前在該計算設備上執行的一應用程式是否是潛在地具有惡意的包括：

分析以下各項中的至少一項：對與存取該計算設備的資源相對應的該一或多個目標應用程式的一許可，以及儲存的指示該一或多個目標應用程式的先前活動的活動資料。

【第19項】 如請求項15之計算設備，其中該一或多個資源包括一或多個設備部件和資料中的一項或兩項。

【第20項】 如請求項19之計算設備，其中該一或多個

設備部件包括由一已安裝應用程式、一作業系統、一網路介面、一處理單元、一資料儲存單元、一耦合的設備、一輸出單元、一輸入單元和一感測器組成的該群組中的至少一個成員。

【第21項】 如請求項19之計算設備，其中該計算設備是一行動計算設備，並且該資料包括由一連絡人清單、一儲存的檔案、個人資訊、網路狀況資料、訂閱資訊、位置資訊、系統資訊、已知易損性資訊和感測器資料組成的該群組中的至少一個成員。

【第22項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而回應於決定該目標應用程式潛在地具有惡意來預測該目標應用程式的該觸發條件包括：

評估以下各項中的至少一項：對該目標應用程式的一許可、先前對於該目標應用程式可存取的任何資源，以及儲存的指示該目標應用程式的先前活動的活動資料。

【第23項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而至少部分地基於所預測的該觸發條件來提供該一或多個資源包括以下各項中的至少一項：

至少部分地基於所預測的該觸發條件，調整先前對

於該目標應用程式可見的一資源；及

配置先前對於該目標應用程式不可見的一資源，從而使該資源變得對於該目標應用程式可見。

【第24項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而至少部分地基於所預測的該觸發條件來提供該一或多個資源包括：

至少部分地基於所預測的該觸發條件來建立一虛擬資源，其中該虛擬資源代表並非實際存在於該計算設備中或由該計算設備支援的模仿的一設備部件或資料。

【第25項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而監聽與所提供的該一或多個資源相對應的該目標應用程式的活動包括：

偵測由該目標應用程式進行的一應用程式介面（API）呼叫。

【第26項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作從而至少部分地基於所監聽到的該等活動來決定該目標應用程式是否具有惡意包括：

評估所監聽到的該等活動和儲存的指示該目標應用

程式的先前活動的活動資料。

【第27項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作亦包括：更新儲存的該目標應用程式的活動資料，該活動資料包括關於回應於決定該目標應用程式具有惡意而提供的資源的資訊。

【第28項】 如請求項15之計算設備，其中該處理器被配置有處理器可執行指令以執行操作亦包括：回應於決定該目標應用程式具有惡意來傳輸指示該目標應用程式的該觸發條件的一報告訊息。

【第29項】 一種其上儲存有處理器可執行指令的非暫時性處理器可讀取儲存媒體，該等處理器可執行指令被配置為使一計算設備的一處理器執行包括以下各項的操作：

回應於決定一或多個目標應用程式潛在地具有惡意，預測該一或多個目標應用程式的一觸發條件；

至少部分地基於所預測的該觸發條件，提供一或多個資源；

監聽與所提供的該一或多個資源相對應的該一或多個目標應用程式的活動；及

至少部分地基於所監聽到的該等活動，決定該一或多個目標應用程式中的任何目標應用程式是否是具有

惡意的。

【第30項】　一種計算設備，包括：

用於回應於決定一或多個目標應用程式潛在地具有惡意，預測該一或多個目標應用程式的一觸發條件的構件；

用於至少部分地基於所預測的該觸發條件，提供一或多個資源的構件；

用於監聽與所提供的該一或多個資源相對應的該一或多個目標應用程式的活動的構件；及

用於至少部分地基於所監聽到的該等活動，決定該一或多個目標應用程式中的任何目標應用程式是否具有惡意的構件。

【發明圖式】

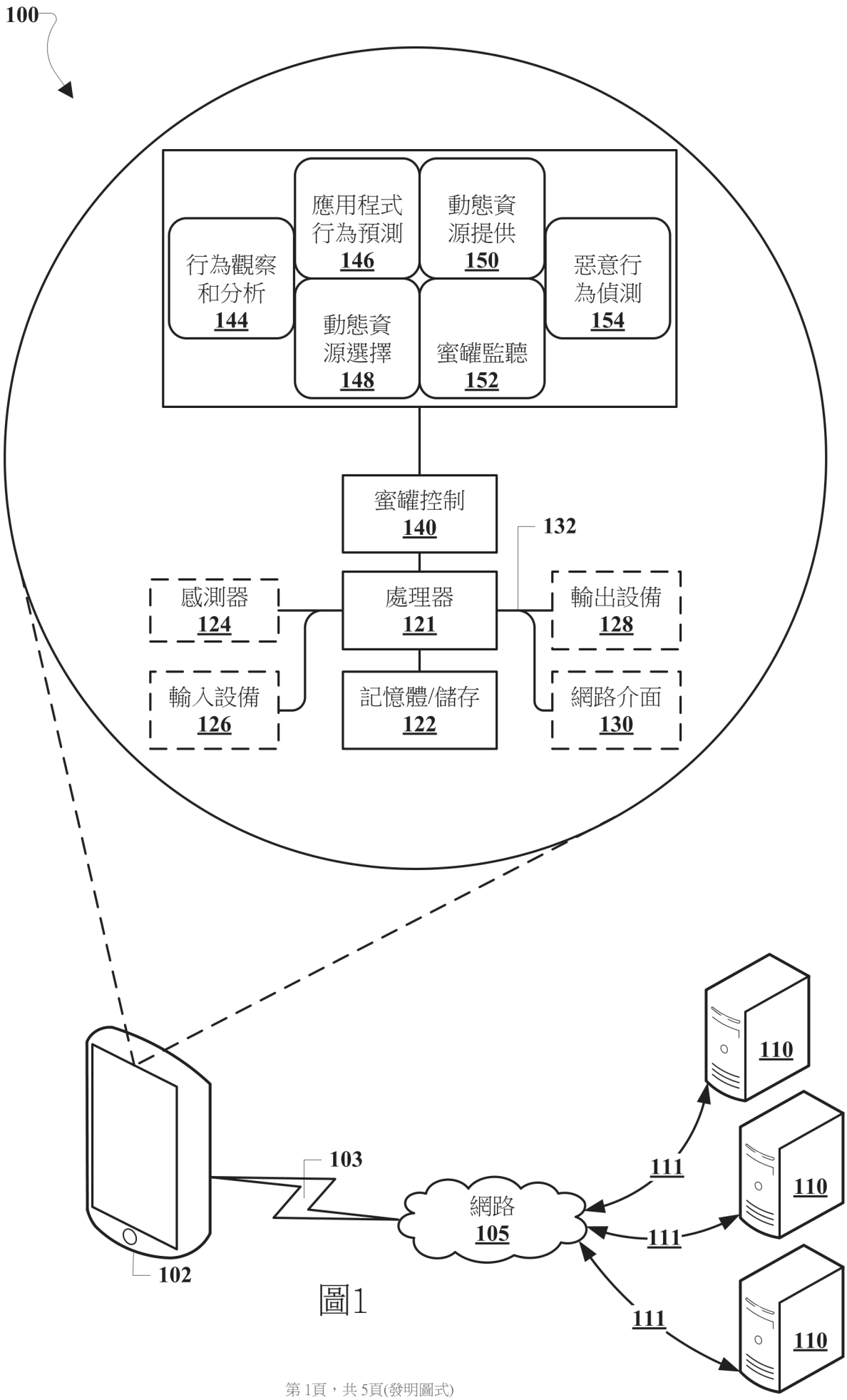
100
應用程式
行為預測
146
動態資
源提供
150
行為觀察
和分析
144
惡意行
為偵測
154
動態資
源選擇
148
蜜罐監聽
152
蜜罐控制
140
132
感測器
124
處理器
121
輸出設備
128
輸入設備
126
記憶體/儲存
122
網路介面
130
110
110
110
111
111
111
103
網路
105
102

圖1

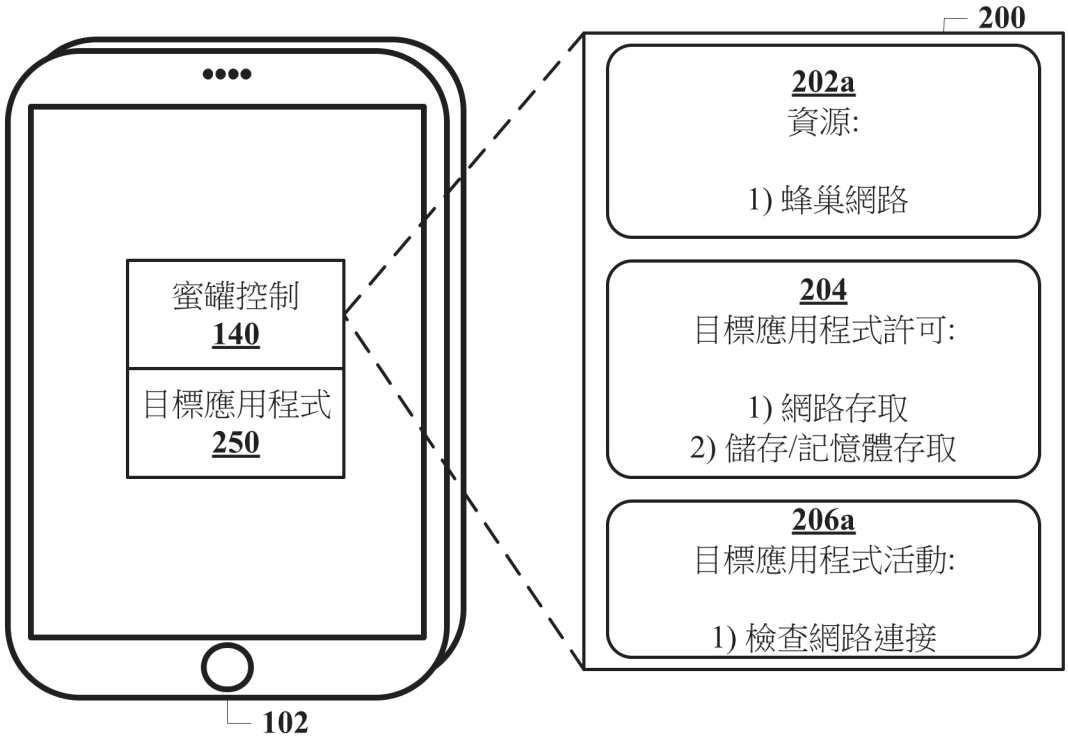
200
202a
資源:
1) 蜂巢網路
204
目標應用程式許可:
1) 網路存取
2) 儲存/記憶體存取
206a
目標應用程式活動:
1) 檢查網路連接
蜜罐控制
140
目標應用程式
250
102

圖2

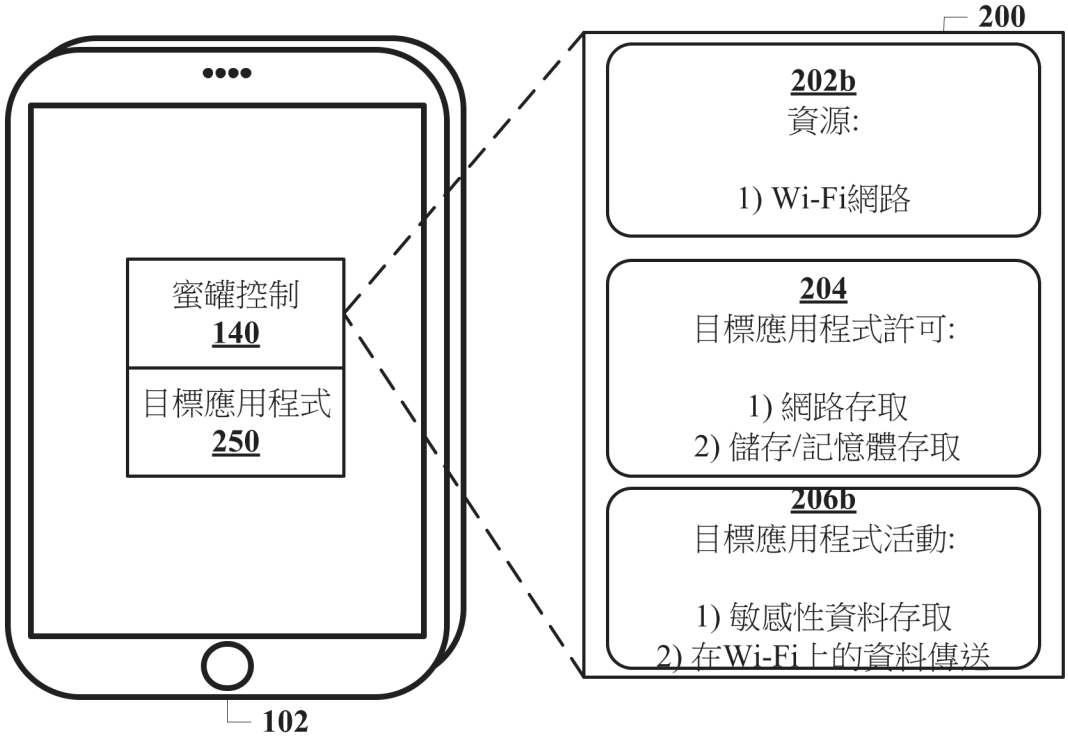
200
202b
資源:
1) Wi-Fi網路
204
目標應用程式許可:
1) 網路存取
2) 儲存/記憶體存取
206b
目標應用程式活動:
1) 敏感性資料存取
2) 在Wi-Fi上的資料傳送
蜜罐控制
140
目標應用程式
250
102

圖3

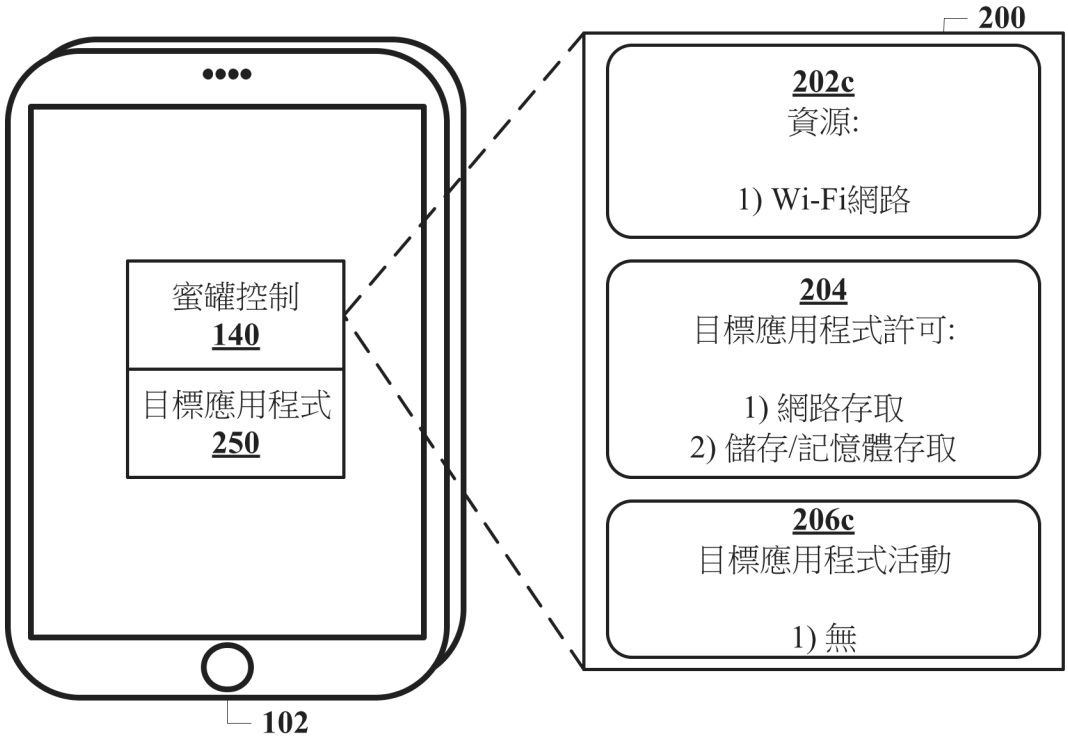
200
202c
資源:
1) Wi-Fi網路
204
目標應用程式許可:
1) 網路存取
2) 儲存/記憶體存取
206c
目標應用程式活動
1) 無
蜜罐控制
140
目標應用程式
250
102

圖4

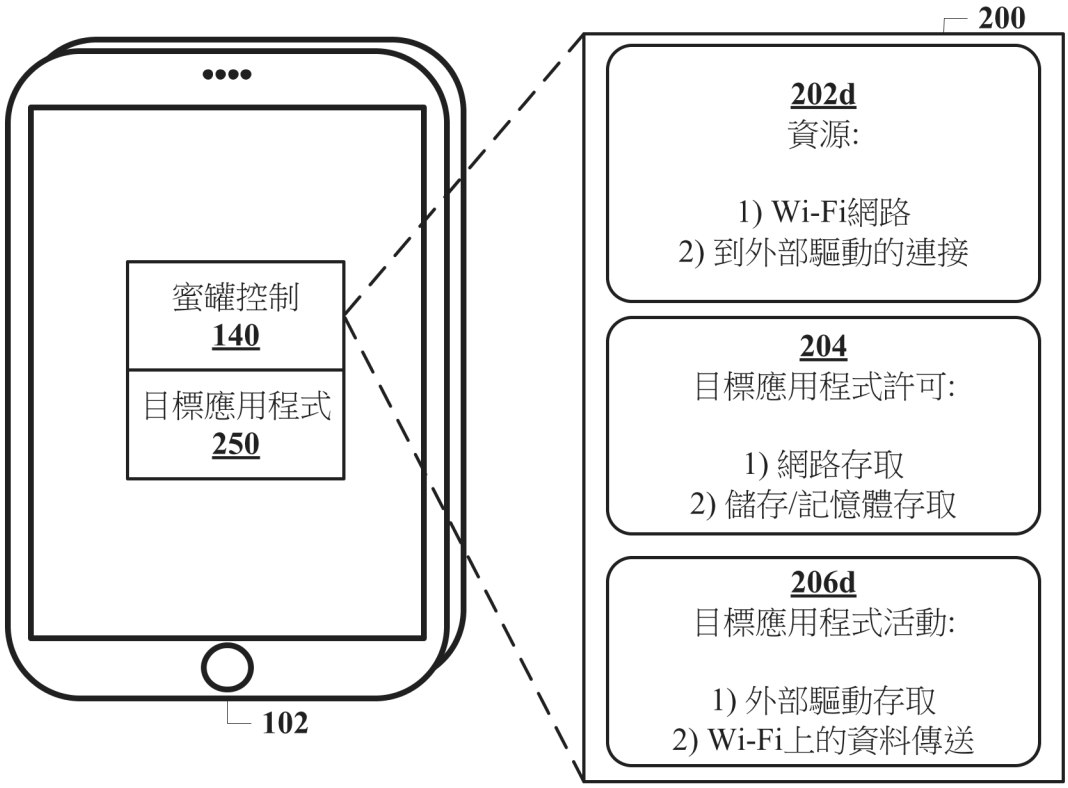
200
202d
資源:
1) Wi-Fi網路
2) 到外部驅動的連接
204
目標應用程式許可:
1) 網路存取
2) 儲存/記憶體存取
206d
目標應用程式活動:
1) 外部驅動存取
2) Wi-Fi上的資料傳送
蜜罐控制
140
目標應用程式
250
102

圖5

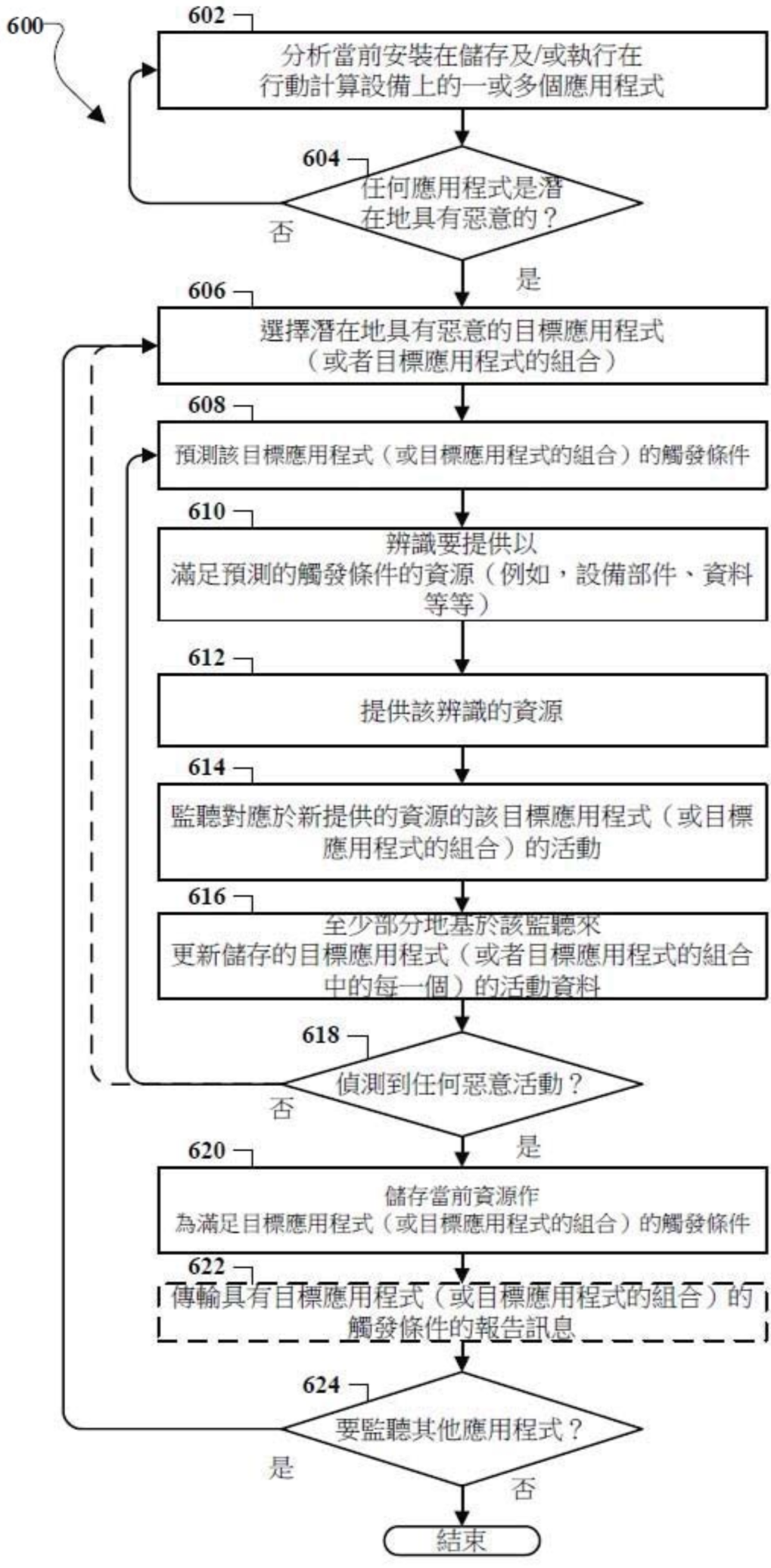
600
602
分析當前安裝在儲存及/或執行在行動計算設備上的一或多個應用程式
604
任何應用程式是潛在地具有惡意的？
否
是
606
選擇潛在地具有惡意的目標應用程式（或者目標應用程式的組合）
608
預測該目標應用程式（或目標應用程式的組合）的觸發條件
610
辨識要提供以滿足預測的觸發條件的資源（例如，設備部件、資料等等）
612
提供該辨識的資源
614
監聽對應於新提供的資源的該目標應用程式（或目標應用程式的組合）的活動
616
至少部分地基於該監聽來更新儲存的目標應用程式（或者目標應用程式的組合中的每一個）的活動資料
618
偵測到任何惡意活動？
否
是
620
儲存當前資源作為滿足目標應用程式（或目標應用程式的組合）的觸發條件
622
傳輸具有目標應用程式（或目標應用程式的組合）的觸發條件的報告訊息
624
要監聽其他應用程式？
是
否
結束

圖6

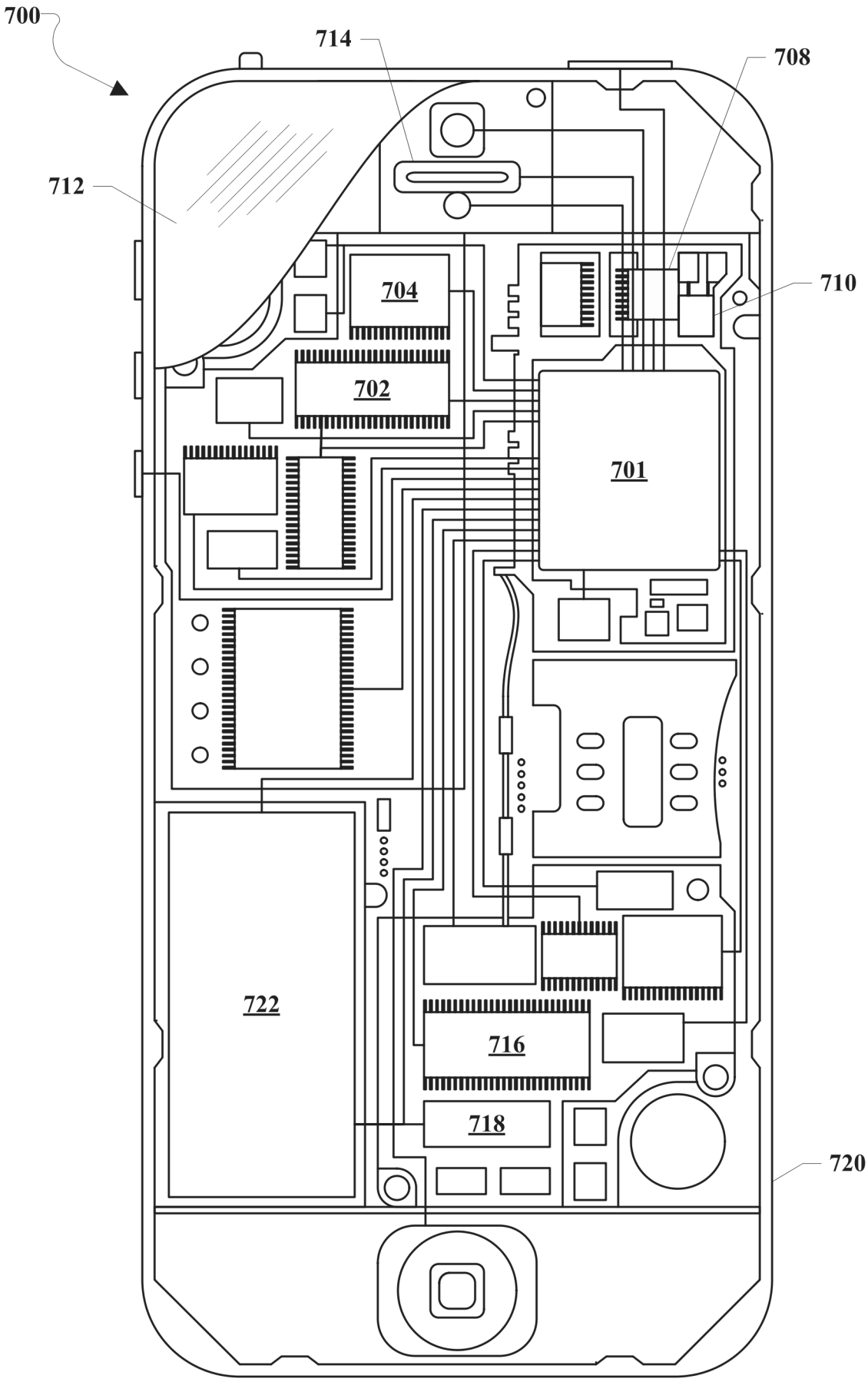

圖7