(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 201346628 A
(43)公開日： 中華民國 102 (2013) 年 11 月 16 日

(21)申請案號：101116554 (22)申請日： 中華民國 101 (2012) 年 05 月 09 日
(51)Int. Cl.： *G06F21/53 (2013.01)* *G06F9/455 (2006.01)*
H04L12/24 (2006.01)
(71)申請人：國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號
(72)發明人：許家維 HSU, CHIAWEI (TW) ；李秉翰 LI, BINGHAN (TW) ；謝續平 SHIEH, SHIUHPYNG (TW)
(74)代理人：蔡坤財；李世章
申請實體審查：有 申請專利範圍項數：10 項 圖式數：4 共 26 頁

(54)名稱

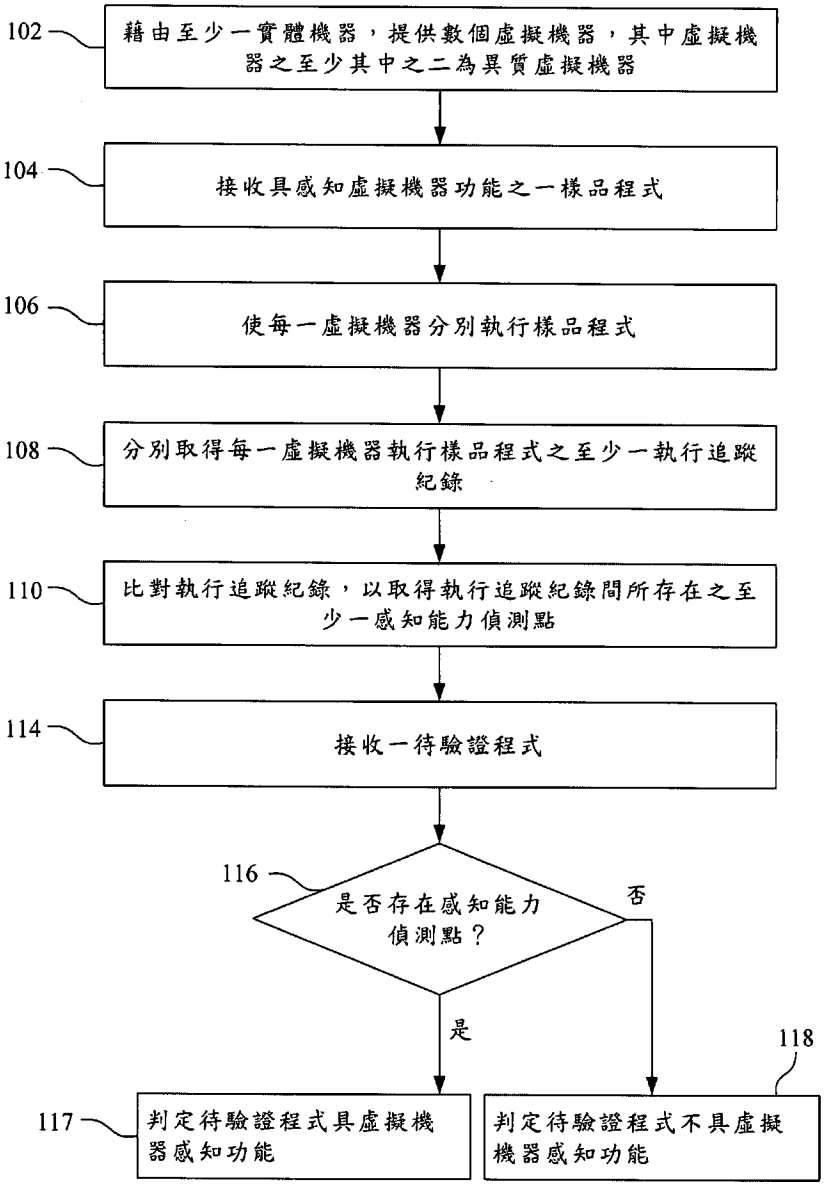
具虛擬機器感知能力程式之偵測方法以及系統

METHOD AND SYSTEM FOR DETECTING PROGRAM WITH VM AWARE ABILITY

(57)摘要

一種具虛擬機器感知能力程式之偵測方法包含以下步驟：藉由至少一實體機器，提供數個虛擬機器。其中，虛擬機器之至少其中之二為異質虛擬機器。接收具感知虛擬機器功能之一樣品程式。使每一虛擬機器分別執行樣品程式。分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄。比對執行追蹤紀錄，以取得執行追蹤紀錄間所存在之至少一感知能力偵測點。接收一待驗證程式。判斷待驗證程式是否存在感知能力偵測點。其中，在待驗證程式存在感知能力偵測點時，判定待驗證程式具虛擬機器感知功能。

100：具虛擬機器感知能力程式之偵測方法
102 ～ 118：步驟



第 1 圖

201346628

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101116554

※申請日：101. 5. 09　　※IPC 分類：G06F 21/53 (2013.01)
G06F 9/455 (2006.01)
H04L 12/54 (2006.01)

一、發明名稱：（中文/英文）

具虛擬機器感知能力程式之偵測方法以及系統

METHOD AND SYSTEM FOR DETECTING PROGRAM WITH VM AWARE ABILITY

二、中文發明摘要：

一種具虛擬機器感知能力程式之偵測方法包含以下步驟：藉由至少一實體機器，提供數個虛擬機器。其中，虛擬機器之至少其中之二為異質虛擬機器。接收具感知虛擬機器功能之一樣品程式。使每一虛擬機器分別執行樣品程式。分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄。比對執行追蹤紀錄，以取得執行追蹤紀錄間所存在之至少一感知能力偵測點。接收一待驗證程式。判斷待驗證程式是否存在感知能力偵測點。其中，在待驗證程式存在感知能力偵測點時，判定待驗證程式具虛擬機器感知功能。

三、英文發明摘要：

A method for detecting a program with a virtual machine (VM) aware ability includes the following steps: several VMs are provided through at least one physical machine. Wherein, at least two of the VMs are heterogeneous. A

sampling program with a VM aware ability is received. Each of the VMs is driven to execute the sampling program respectively. At least one execution trace record, which records information about each VM executing the sampling program. The execution trace records are compared to obtain at least one check point between the execution trace records. A program to be checked is received. Determine if the program to be checked includes the check point. Wherein, if the program to be checked includes the check point, the program to be checked is determined as the one with the VM aware ability.

四、指定代表圖：

(一)本案指定代表圖為：第 1 圖。

(二)本代表圖之元件符號簡單說明：

100：具虛擬機器感知能力程式之偵測方法

102～118：步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種具虛擬機器感知能力程式之偵測方法以及系統，且特別是有關於一種藉由異質之多個虛擬機器，偵測具虛擬機器感知能力程式之方法以及系統。

【先前技術】

隨著網路的普及，近年來越來越多網路安全事件頻繁發生，如網路詐騙活動和資料竊取等。其中，惡意程式（Malware），例如:病毒、開後門程式、間諜軟件、特洛依木馬和蠕蟲等，常常為這類網路安全事件的罪魁禍首。因此，如何檢測惡意程式是一個非常重要的網路安全問題。

先前技術中，惡意程式檢測方法主要有兩種，一個是靜態分析（程式碼分析），另一個是動態分析(惡意程式行為分析)。其中，動態分析可監測遭惡意程式感染的系統以及分析網路流量，並找出遭惡意改變的檔案和登錄檔。

由於在虛擬機器（virtual machine，VM）提供的執行環境下執行惡意程式，惡意程式只會損害到虛擬作業系統或虛擬機器，並不會造成真實的作業系統或真實環境的損害，因此藉由虛擬機器提供的執行環境廣泛被認為是一個有效的惡意行為分析機制。然而，多半是在進行惡意程式分析時，惡意程式才會於虛擬機器內執行，因此並不會獲得太多有用的信息。為了避免被分析，演化過後的惡意程式常附帶感知虛擬機器之功能。若辨識出其所在的執行環境為虛擬機器所提供時，這些惡意軟體會隱藏自己真正的

意圖來規避虛擬機器的分析，混淆其分析結果。

【發明內容】

因此，本發明之一態樣是在提供一種具虛擬機器（virtual machine，VM）感知能力程式之偵測方法，用以在多台異質之虛擬機器執行具虛擬機器感知能力之程式，以取得其執行追蹤（execution trace）紀錄，並根據其執行追蹤紀錄找出感知能力偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。具虛擬機器感知能力程式之偵測方法可實作為一電腦程式，並儲存於一電腦可讀取記錄媒體。於是，電腦存取上述電腦可讀取紀錄媒體後，可執行具虛擬機器感知能力程式之偵測方法。具虛擬機器感知能力程式之偵測方法包含以下步驟：

（a）藉由至少一實體機器，提供數個虛擬機器。其中，所提供之虛擬機器之至少其中之二為異質（heterogeneous）虛擬機器。

（b）接收具感知虛擬機器功能之一樣品程式。

（c）使每一虛擬機器分別執行樣品程式。

（d）分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄。

（e）比對執行追蹤紀錄，以取得執行追蹤紀錄間所存在之至少一感知能力偵測點。

（f）接收一待驗證程式。

（g）判斷待驗證程式是否存在感知能力偵測點。其中，在待驗證程式存在感知能力偵測點時，判定該待驗證

5

程式具虛擬機器感知功能。

本發明之另一態樣是在提供一種具虛擬機器感知能力程式之偵測系統，用以在多台異質之虛擬機器執行具虛擬機器感知能力之程式，以取得其執行追蹤紀錄，並根據其執行追蹤紀錄找出感知能力偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。具虛擬機器感知能力程式之偵測系統包含相互建立連結之一程式輸入元件以及至少一處理元件。處理元件包含一虛擬機器提供模組、一程式接收模組、一程式執行模組、一紀錄取得模組、一比對模組以及一偵測點判斷模組。虛擬機器提供模組提供數個虛擬機器，其中，所提供之虛擬機器之至少其中之二為異質虛擬機器。程式接收模組透過程式輸入元件，接收一樣品程式以及一待驗證程式。其中，樣品程式具感知虛擬機器功能。程式執行模組驅動每一虛擬機器分別執行樣品程式。紀錄取得模組分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄。比對模組比對各執行追蹤紀錄，以取得各執行追蹤紀錄間所存在之至少一感知能力偵測點。偵測點判斷模組判斷待驗證程式是否存在感知能力偵測點。其中，在待驗證程式存在感知能力偵測點時，處理元件判定待驗證程式具虛擬機器感知功能。

應用本發明具有下列優點。可藉由多個異質虛擬機器，找到程式進行虛擬機器感知之偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。尤其，可在找到偵測點後，可更精確的針對感知虛擬機器用之偵測點，判斷待驗證程式是否為惡意程式，避免惡意程式因為感測到其

處於虛擬機器環境，而隱藏其惡意行為、無法被偵測。

【實施方式】

以下將以圖式及詳細說明清楚說明本發明之精神，任何所屬技術領域中具有通常知識者在瞭解本發明之較佳實施例後，當可由本發明所教示之技術，加以改變及修飾，其並不脫離本發明之精神與範圍。

請參照第 1 圖，其為依照本發明一實施方式的一種具虛擬機器（virtual machine，VM）感知能力程式之偵測方法之流程圖。在具虛擬機器感知能力程式之偵測方法中，在多台異質之虛擬機器執行具虛擬機器感知能力之程式，以取得其執行追蹤（execution trace）紀錄，並根據其執行追蹤紀錄找出感知能力偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。具虛擬機器感知能力程式之偵測方法可實作為一電腦程式，並儲存於一電腦可讀取記錄媒體中，而使電腦讀取此記錄媒體後執行具虛擬機器感知能力程式之偵測方法。電腦可讀取記錄媒體可為唯讀記憶體、快閃記憶體、軟碟、硬碟、光碟、隨身碟、磁帶、可由網路存取之資料庫或熟悉此技藝者可輕易思及具有相同功能之電腦可讀取記錄媒體。

具虛擬機器感知能力程式之偵測方法 100 包含以下步驟：

在步驟 102 中，藉由至少一實體機器，提供數個虛擬機器。其中，所提供之虛擬機器之至少其中之二為異質（heterogeneous）虛擬機器。在本發明之一實施例中，所

謂異質之虛擬機器係指執行於不同虛擬機器平台者。

在步驟 104 中，接收具感知虛擬機器功能之一樣品程式。

在步驟 106 中，使每一虛擬機器分別執行樣品程式。

於是，在步驟 108 中，分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄。在本發明之一實施例中，可使各虛擬機器分別執行 1 次樣品程式（步驟 106），以分別取得各虛擬機器執行樣品程式之一筆執行追蹤紀錄（步驟 108）。在本發明之另一實施例中，可使各虛擬機器分別執行多次樣品程式（步驟 106），以分別取得各虛擬機器執行樣品程式之多筆執行追蹤紀錄（步驟 108）。在本發明之其他實施例中，可使各虛擬機器分別執行樣品程式不同次數（步驟 106），以分別取得各虛擬機器執行樣品程式之不同筆數之執行追蹤紀錄（步驟 108），並不限於本揭露。此外，於步驟 108 所取得之執行追蹤紀錄係紀錄各虛擬機器執行樣品程式時，於指令階級（instruction level）下之資訊，如所執行之作業碼（operation code）、指令執行時所儲存之暫存器（register）位址或其他指令階級下之資訊。

在步驟 110 中，比對執行追蹤紀錄，以取得執行追蹤紀錄間所存在之至少一感知能力偵測點。於是，接下來可根據感知能力偵測點，進行程式是否具虛擬機器感知功能之判斷。

在步驟 114 中，接收一待驗證程式。

在步驟 116 中，判斷待驗證程式是否存在感知能力偵測點。

在步驟 117 中，在待驗證程式存在感知能力偵測點時，判定待驗證程式具虛擬機器感知功能。

此外，在步驟 118 中，在待驗證程式不存在感知能力偵測點時，判定待驗證程式不具虛擬機器感知功能。如此一來，可藉由多個異質虛擬機器找到感知能力偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。

參照第 2 圖，其為各虛擬機器執行樣品程式所分別取得之至少一執行追蹤紀錄（步驟 108）之一實施例。在此實施例中，執行追蹤紀錄 211～213 為虛擬機器 210 執行樣品程式時所取得；而執行追蹤紀錄 221～223 為與虛擬機器 210 異質之虛擬機器 220 執行同一樣品程式時所取得。於是，比對執行追蹤紀錄，以取得執行追蹤紀錄間所存在之至少一感知能力偵測點（步驟 110）可包含以下步驟：尋找由異質之虛擬機器 210、220 執行所得之執行追蹤紀錄 211～213、221～223 中，相異之至少一相異指令執行記錄。其中，213 係執行於 0x401216，不同於 223 係執行於 0x401218。因此，使相異指令執行記錄 213、223 執行前之前一筆先前執行紀錄 212、222，作為感知能力偵測點。於是，在收到待驗證程式（步驟 114）時，由虛擬機器 210、220 執行待驗證程式，判斷是否待驗證程式程式中是否有如 212、222 之感知能力偵測點，其接下來將執行相異之紀錄（如 213、223）（步驟 116）。如果待驗證程式有此感知能力偵測點時，判定此待驗證程式具虛擬機器感知功能（步驟 117）。此外，在本發明之另一些實施例中，可用聯集（∪）之邏輯運算子算出個別執行追蹤紀錄所包含之已執行指令

集（或稱 code coverage）。於是，接下來可針對各已執行指令集間之差異指令，進行感知能力偵測點之尋找。如此一來，可藉由聯集（∪）減少執行追蹤紀錄間進行比對所需之運算量。

參照第 3 圖，其為各虛擬機器執行樣品程式所分別取得之至少一執行追蹤紀錄（步驟 108）之另一實施例。在此實施例中，執行追蹤紀錄 311～315 為虛擬機器 310 執行樣品程式時所取得；而執行追蹤紀錄 321 → 322 → 323a → 324 → 325 以及 321 → 322 → 323b → 324 → 325 為與虛擬機器 310 異質之虛擬機器 320 執行同一樣品程式多次時所取得。於是，具虛擬機器感知能力程式之偵測方法 100 更可進一步將不確定點移除，進一步提高本發明對於感知能力偵測點之偵測正確率。因此，可尋找由同一虛擬機器 320 執行所得之多筆執行追蹤紀錄中相異之至少一相異指令執行記錄 323a、323b，作為不確定點。此外，由另一虛擬機器 310 執行樣品程式所得之對應執行紀錄 313，亦被視為不確定點。於是，在收到待驗證程式（步驟 114）時，可判斷待驗證程式是否存在不確定點（如 312 執行後之不確定點 313，或者是 322 執行後之不確定點 323a 或 323b）。當待驗證程式存在不確定點時，在取得感知能力偵測點之步驟前，移除待驗證程式中之不確定點（如 313、323a、323b）。如此一來，可避免具虛擬機器感知能力之判斷受不確定點影響造成誤判，因而可提高程式是否具虛擬機器感知能力之判斷正確率。

此外，具虛擬機器感知能力程式之偵測方法 100 可進

一步在待驗證程式存在感知能力偵測點時，自感知能力偵測點，分析並判斷待驗證程式是否為惡意程式。如此一來，由於已知程式將執行不同行為之感知能力偵測點，因此可進一步針對感知能力偵測點，判斷其所執行之不同行為是否為惡意程式之行為。然而，在本發明之其他實施例中，亦可藉由其他方式，自感知能力偵測點，分析並判斷具感知能力偵測點之待驗證程式是否為惡意程式。於是，即使待驗證之程式具虛擬機器感知能力，仍可藉由本發明之技術特徵，判斷出其是否為惡意程式。換言之，可避免惡意程式因為感測到其處於虛擬機器環境，而隱藏其惡意行為、無法被偵測。

請參照第 4 圖，其繪示依照本發明一實施方式的一種具虛擬機器感知能力程式之偵測系統之功能方塊圖。具虛擬機器感知能力程式之偵測系統在多台異質之虛擬機器執行具虛擬機器感知能力之程式，以取得其執行追蹤紀錄，並根據其執行追蹤紀錄找出感知能力偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。

具虛擬機器感知能力程式之偵測系統 400 包含相互建立連結之一程式輸入元件 410 以及至少一處理元件 420。在本發明之一些實施例中，程式輸入元件 410 可為具有線或無線資料傳輸介面之硬體元件。然而，在其他實施例中，程式輸入元件 410 可為其他可透過其輸入程式之硬體元件，並不限於本揭露。

至少一處理元件 420 包含一虛擬機器提供模組 421、一程式接收模組 422、一程式執行模組 423、一紀錄取得模

組 424、一比對模組 425 以及一偵測點判斷模組 426。其中，模組 421～426 可實作於單一處理元件或分散式的實作於多個處理元件，並不限於本揭露書。

虛擬機器提供模組 421 提供數個虛擬機器，其中，所提供之虛擬機器之至少其中之二為異質虛擬機器。在本發明之一實施例中，虛擬機器提供模組 421 可應用不同虛擬機器平台，而提供異質之虛擬機器。

程式接收模組 422 透過程式輸入元件 410，接收一樣品程式以及一待驗證程式。其中，樣品程式具感知虛擬機器功能。程式執行模組 423 驅動虛擬機器提供模組 421 所提供之每一虛擬機器分別執行樣品程式。於是，紀錄取得模組 424 分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄。在本發明之一實施例中，程式執行模組 423 可驅動各虛擬機器分別執行 1 次樣品程式，以供紀錄取得模組 424 分別取得各虛擬機器執行樣品程式之一筆執行追蹤紀錄。在本發明之另一實施例中，程式執行模組 423 可驅動各虛擬機器分別執行多次樣品程式，以供紀錄取得模組 424 分別取得各虛擬機器執行樣品程式之多筆執行追蹤紀錄。在本發明之其他實施例中，程式執行模組 423 可驅動各虛擬機器分別執行樣品程式不同次數，以供紀錄取得模組 424 分別取得各虛擬機器執行樣品程式之不同筆數之執行追蹤紀錄，並不限於本揭露。此外，紀錄取得模組 424 係紀錄各虛擬機器執行樣品程式時，於指令階級下之資訊，如所執行之作業碼、指令執行時所儲存之暫存器位址或其他指令階級下之資訊。

比對模組 425 比對各執行追蹤紀錄，以取得各執行追蹤紀錄間所存在之至少一感知能力偵測點。於是，接下來偵測點判斷模組 426 判斷待驗證程式是否存在感知能力偵測點。其中，在待驗證程式存在感知能力偵測點時，處理元件 420 判定待驗證程式具虛擬機器感知功能。如此一來，可藉由虛擬機器提供模組 421 所提供之多個異質虛擬機器，找到感知能力偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。

在本發明之一實施例中，比對模組 425 可包含一尋找器 425a。尋找器 425a 可尋找由異質之多個虛擬機器執行所得之執行追蹤紀錄中，相異之至少一相異指令執行記錄。其中，比對模組 425 使相異指令執行記錄執行前之前一筆先前執行紀錄，作為至少一感知能力偵測點。於是，偵測點判斷模組 426 可藉由判斷待驗證程式中是否有其接下來將執行上述相異之紀錄之感知能力偵測點，判斷待驗證程式是否具虛擬機器感知功能。此外，在本發明之一些實施例中，尋找器 425a 可用聯集（∪）之邏輯運算子算出個別執行追蹤紀錄所包含之已執行指令集（或稱 code coverage）。於是，接下來尋找器 425a 可針對各已執行指令集間之差異指令，進行感知能力偵測點之尋找。如此一來，可藉由聯集（∪）減少執行追蹤紀錄間進行比對所需之運算量。

在本發明之一實施例中，處理元件 420 更可包含一尋找模組 427 以及一不確定點判斷模組 428。程式執行模組 423 驅動虛擬機器之至少其中之一執行樣品程式複數次

時，尋找模組 427 可尋找由同一虛擬機器執行所得之多筆執行追蹤紀錄中相異之至少一相異指令執行記錄，作為一不確定點。於是，不確定點判斷模組 428 可判斷待驗證程式是否存在不確定點。當判定待驗證程式存在不確定點時，在偵測點判斷模組 426 執行前，處理元件 420 移除待驗證程式中之不確定點。如此一來，可避免具虛擬機器感知能力之判斷受不確定點影響造成誤判，因而可提高程式是否具虛擬機器感知能力之判斷正確率。

此外，處理元件 420 更可包含一惡意程式處理模組 429。在待驗證程式存在感知能力偵測點時，惡意程式處理模組 429 自感知能力偵測點，分析並判斷待驗證程式是否為惡意程式。如此一來，由於已知程式將執行不同行為之感知能力偵測點，因此惡意程式處理模組 429 可進一步針對感知能力偵測點，判斷其所執行之不同行為是否為惡意程式之行為。然而，在本發明之其他實施例中，惡意程式處理模組 429 亦可藉由其他方式，自感知能力偵測點分析並判斷具感知能力偵測點之待驗證程式是否為惡意程式。於是，即使待驗證之程式具虛擬機器感知能力，仍可藉由本發明之技術特徵，判斷出其是否為惡意程式。換言之，可避免惡意程式因為感測到其處於虛擬機器環境，而隱藏其惡意行為、無法被偵測。

應用本發明具有下列優點。可藉由多個異質虛擬機器，找到程式進行虛擬機器感知之偵測點，作為判斷其他程式是否具虛擬機器感知能力之依據。尤其，可在找到偵測點後，可更精確的針對感知虛擬機器用之偵測點，判斷

待驗證程式是否為惡意程式，避免惡意程式因為感測到其處於虛擬機器環境，而隱藏其惡意行為、無法被偵測。

雖然本發明已以實施方式揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作各種之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

為讓本發明之上述和其他目的、特徵、優點與實施例能更明顯易懂，所附圖式之說明如下：

第 1 圖為依照本發明一實施方式的一種具虛擬機器感知能力程式之偵測方法之流程圖。

第 2 圖為各虛擬機器執行樣品程式所分別取得之至少一執行追蹤紀錄（步驟 108）之一實施例。

第 3 圖為各虛擬機器執行樣品程式所分別取得之至少一執行追蹤紀錄（步驟 108）之另一實施例。

第 4 圖繪示依照本發明一實施方式的一種具虛擬機器感知能力程式之偵測系統之功能方塊圖。

【主要元件符號說明】

100：具虛擬機器感知能力程式之偵測方法
102～118：步驟
210、220、310、320：虛擬機器
421：目標內容層次偏移空間
422：程式接收模組
423：程式執行模組
424：紀錄取得模組
425：比對模組

211～213、221～223、311～315、321～325：執行追蹤紀錄

400：具虛擬機器感知能力程式之偵測系統

410：程式輸入元件

420：處理元件

425a：尋找器

426：偵測點判斷模組

426：偵測點判斷模組

427：尋找模組

428：不確定點判斷模組

429：惡意程式處理模組

七、申請專利範圍：

1. 一種具虛擬機器（virtual machine，VM）感知能力程式之偵測方法，包含：

（a）藉由至少一實體機器，提供複數個虛擬機器，其中該些虛擬機器之至少其中之二為異質（heterogeneous）虛擬機器；

（b）接收具感知虛擬機器功能之一樣品程式；

（c）使每一該些虛擬機器分別執行該樣品程式；

（d）分別取得每一該些虛擬機器執行該樣品程式之至少一執行追蹤（execution trace）紀錄；

（e）比對該些執行追蹤紀錄，以取得該些執行追蹤紀錄間所存在之至少一感知能力偵測點；

（f）接收一待驗證程式；以及

（g）判斷該待驗證程式是否存在該至少一感知能力偵測點，其中在該待驗證程式存在該至少一感知能力偵測點時，判定該待驗證程式具虛擬機器感知功能。

2. 如請求項 1 所述之偵測方法，其中該些虛擬機器中為異質虛擬機器者係執行不同虛擬機器平台。

3. 如請求項 1 所述之偵測方法，其中步驟（e）包含：

尋找由異質之該些虛擬機器執行所得之該些執行追蹤紀錄中，相異之至少一相異指令執行記錄；以及

使該相異指令執行記錄執行前之前一筆先前執行紀

錄，作為該至少一感知能力偵測點。

4. 如請求項1所述之偵測方法，其中：

步驟（c）包含使該些虛擬機器之至少其中之一執行該樣品程式複數次；

該偵測方法更包含：

尋找由同一虛擬機器執行所得之該些執行追蹤紀錄中相異之至少一相異指令執行記錄，作為一不確定點；

判斷該待驗證程式是否存在該不確定點；以及

當該待驗證程式存在該不確定點時，在取得該至少一感知能力偵測點前，移除該待驗證程式中之該不確定點。

5. 如請求項1所述之偵測方法，更包含：

在該待驗證程式存在該至少一感知能力偵測點時，自該至少一感知能力偵測點，分析並判斷該待驗證程式是否為惡意程式。

6. 一種具虛擬機器感知能力程式之偵測系統，包含：

一程式輸入元件；以及

至少一處理元件，與該程式輸入元件建立連結，其中該處理元件包含：

一虛擬機器提供模組，提供複數個虛擬機器，其中該些虛擬機器之至少其中之二為異質虛擬機器；

一程式接收模組，透過該程式輸入元件，接收一樣品程式以及一待驗證程式，其中該樣品程式具感知虛擬機器功能；

一程式執行模組，驅動每一該些虛擬機器分別執行該樣品程式；

一紀錄取得模組，分別取得每一該些虛擬機器執行該樣品程式之至少一執行追蹤紀錄；

一比對模組，比對該些執行追蹤紀錄，以取得該些執行追蹤紀錄間所存在之至少一感知能力偵測點；以及

一偵測點判斷模組，判斷該待驗證程式是否存在該至少一感知能力偵測點，其中在該待驗證程式存在該至少一感知能力偵測點時，該處理元件判定該待驗證程式具虛擬機器感知功能。

7. 如請求項 6 所述之偵測系統，其中該虛擬機器提供模組所提供之該些虛擬機器中為異質虛擬機器者係執行不同虛擬機器平台。

8. 如請求項 6 所述之偵測系統，其中該比對模組包含：

一尋找器，尋找由異質之該些虛擬機器執行所得之該些執行追蹤紀錄中，相異之至少一相異指令執行記錄，其中該比對模組使該相異指令執行記錄執行前之前一筆先前執行紀錄，作為該至少一感知能力偵測點。

9. 如請求項6所述之偵測系統，其中：

該程式執行模組驅動該些虛擬機器之至少其中之一執行該樣品程式複數次；

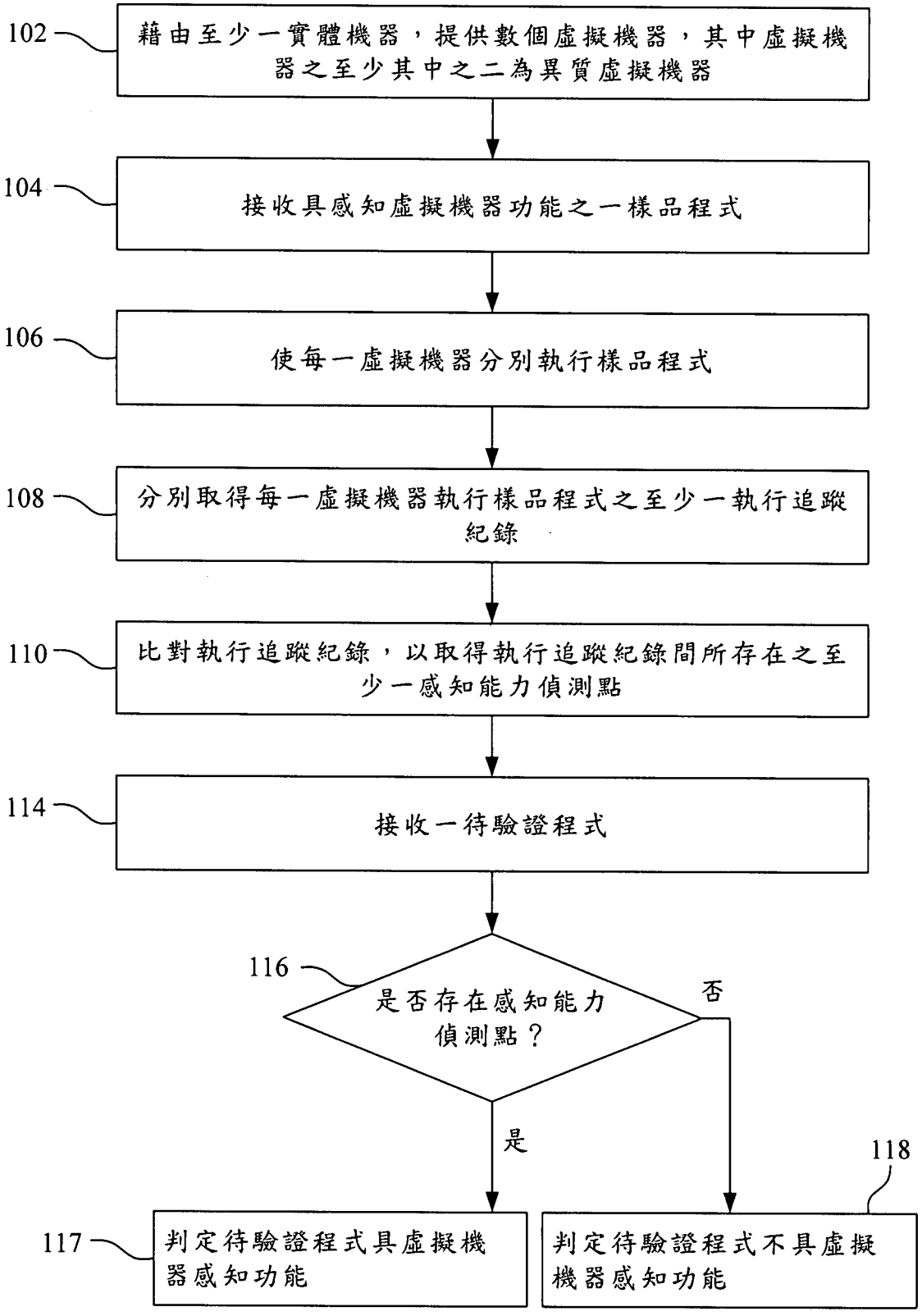
該處理元件更包含：

一尋找模組，尋找由同一虛擬機器執行所得之該些執行追蹤紀錄中相異之至少一相異指令執行記錄，作為一不確定點；以及

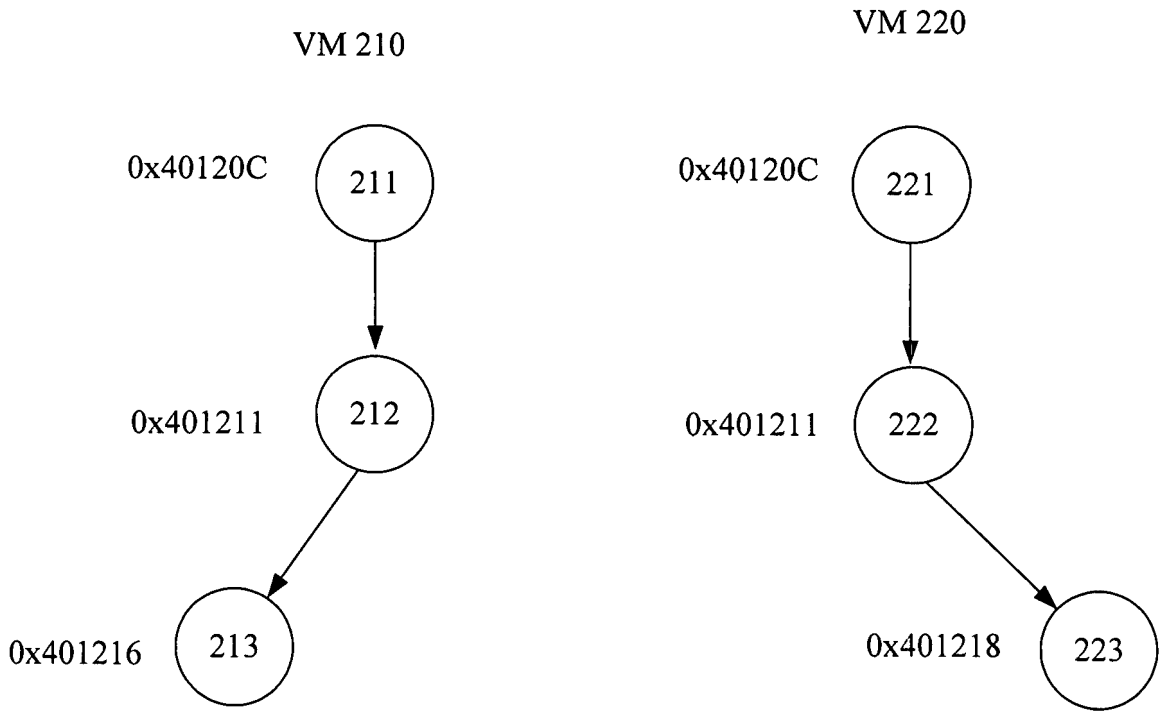
一不確定點判斷模組，判斷該待驗證程式是否存在該不確定點，其中當該待驗證程式存在該不確定點時，在該偵測點判斷模組執行前，該處理元件移除該待驗證程式中之該不確定點。

10. 如請求項6所述之偵測系統，其中該處理元件包含：

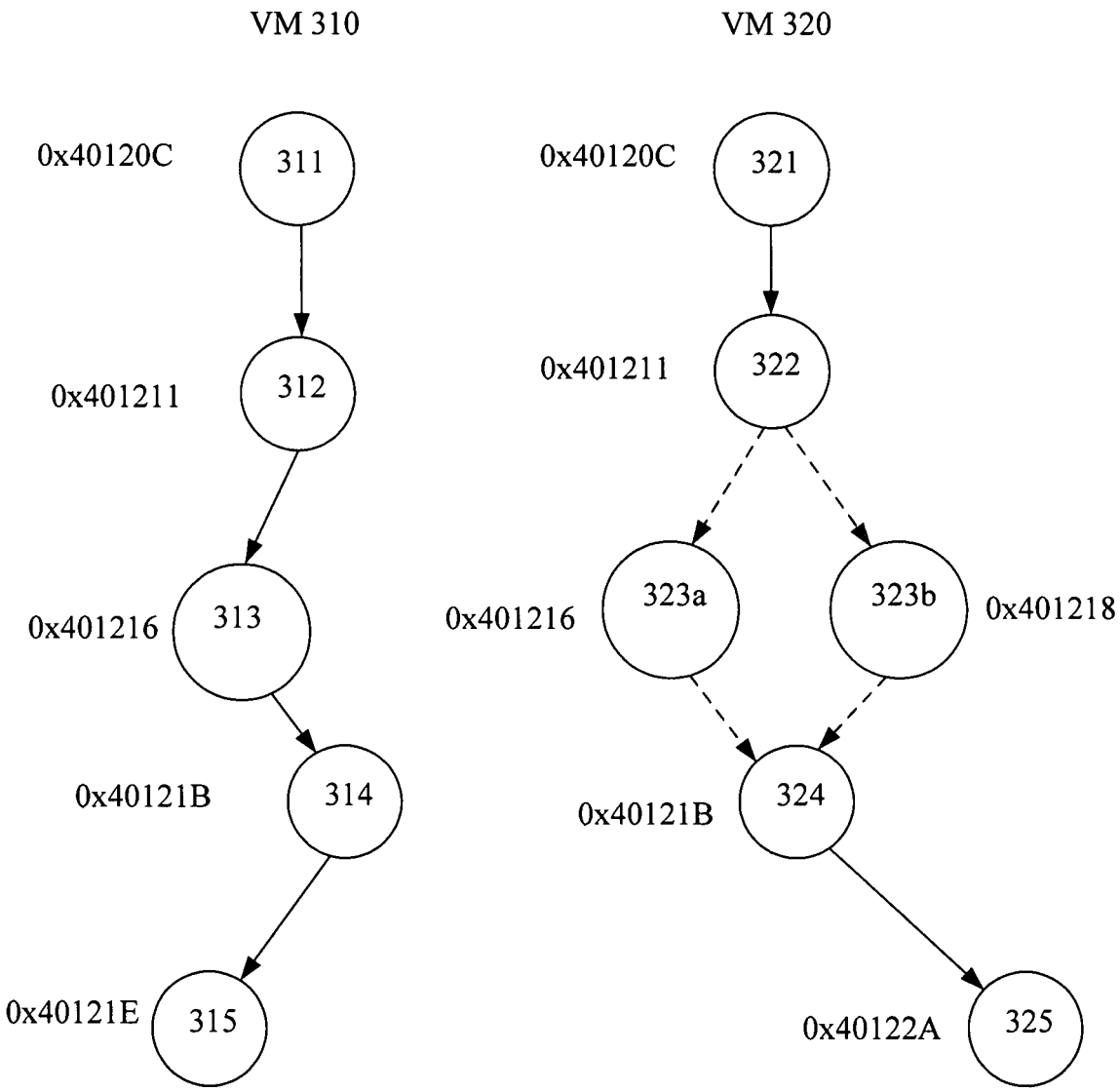
一惡意程式處理模組，在該待驗證程式存在該至少一感知能力偵測點時，自該至少一感知能力偵測點，分析並判斷該待驗證程式是否為惡意程式。


102
藉由至少一實體機器，提供數個虛擬機器，其中虛擬機器之至少其中之二為異質虛擬機器
104
接收具感知虛擬機器功能之一樣品程式
106
使每一虛擬機器分別執行樣品程式
108
分別取得每一虛擬機器執行樣品程式之至少一執行追蹤紀錄
110
比對執行追蹤紀錄，以取得執行追蹤紀錄間所存在之至少一感知能力偵測點
114
接收一待驗證程式
116
是否存在感知能力偵測點？
否
是
117
判定待驗證程式具虛擬機器感知功能
118
判定待驗證程式不具虛擬機器感知功能
100

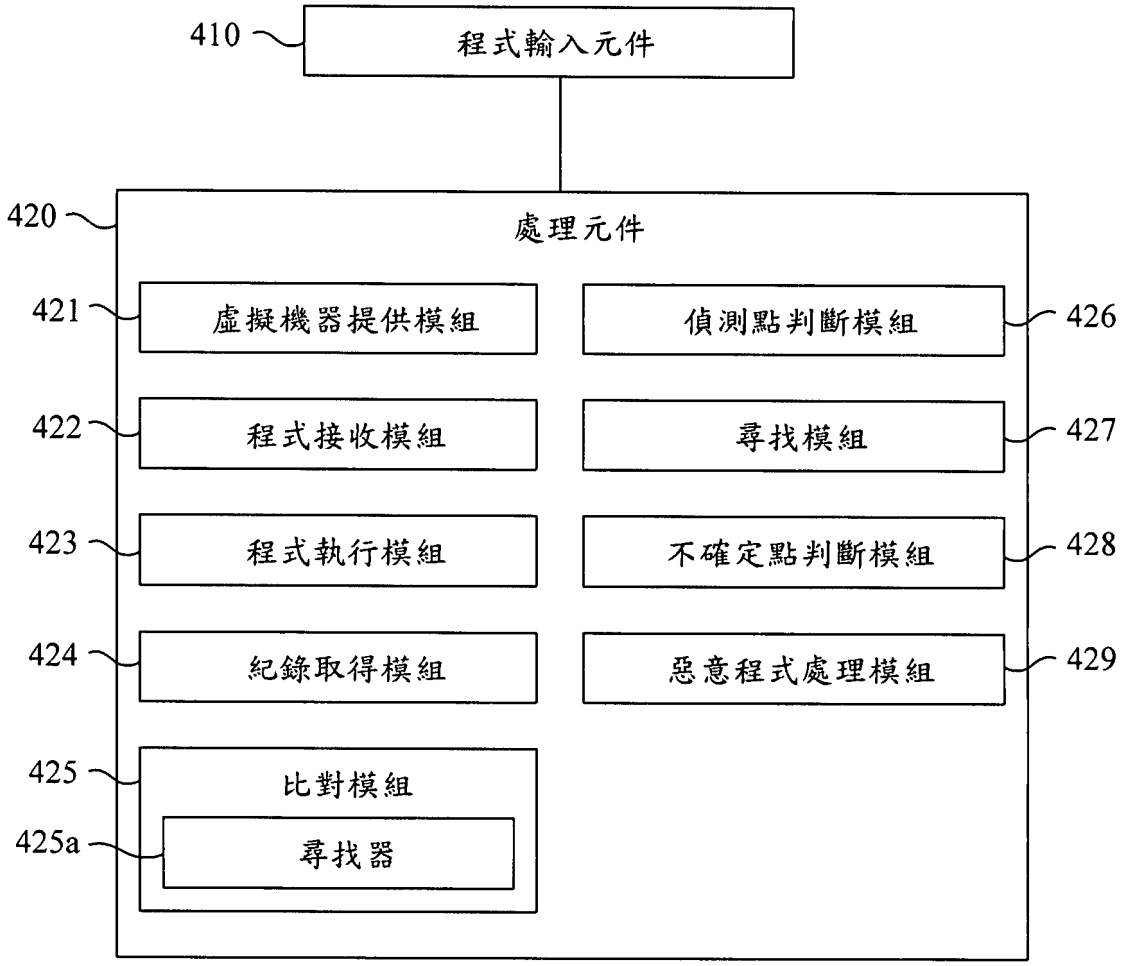
第 1 圖


VM 210
0x40120C
211
0x401211
212
0x401216
213
VM 220
0x40120C
221
0x401211
222
0x401218
223

第 2 圖


VM 310
VM 320
0x40120C
311
0x401211
312
0x401216
313
0x40121B
314
0x40121E
315
0x40120C
321
0x401211
322
0x401216
323a
323b
0x401218
0x40121B
324
0x40122A
325

第 3 圖


410
程式輸入元件
420
處理元件
421
虛擬機器提供模組
422
程式接收模組
423
程式執行模組
424
紀錄取得模組
425
比對模組
425a
尋找器
426
偵測點判斷模組
427
尋找模組
428
不確定點判斷模組
429
惡意程式處理模組

400

第 4 圖