201712545

(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 201712545 A

(43)公開日： 中華民國 106 (2017) 年 04 月 01 日

(21)申請案號：104131390 (22)申請日： 中華民國 104 (2015) 年 09 月 23 日

(51)Int. Cl.： *G06F11/30 (2006.01)* *G06F11/36 (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：謝續平 SHIEH, SHIUHPYNG (TW) ；王繼偉 WANG, CHI WEI (TW) ；王嘉偉 WANG, CHIA WEI (TW) ；許家維 HSU, CHIA WEI (TW)

(74)代理人：陳昭誠

申請實體審查：有 申請專利範圍項數：14 項 圖式數：7 共 30 頁

(54)名稱

自動化探針建構系統及其方法

AUTOMATIC PROBE CONSTRUCTION SYSTEM AND METHOD THEREOF

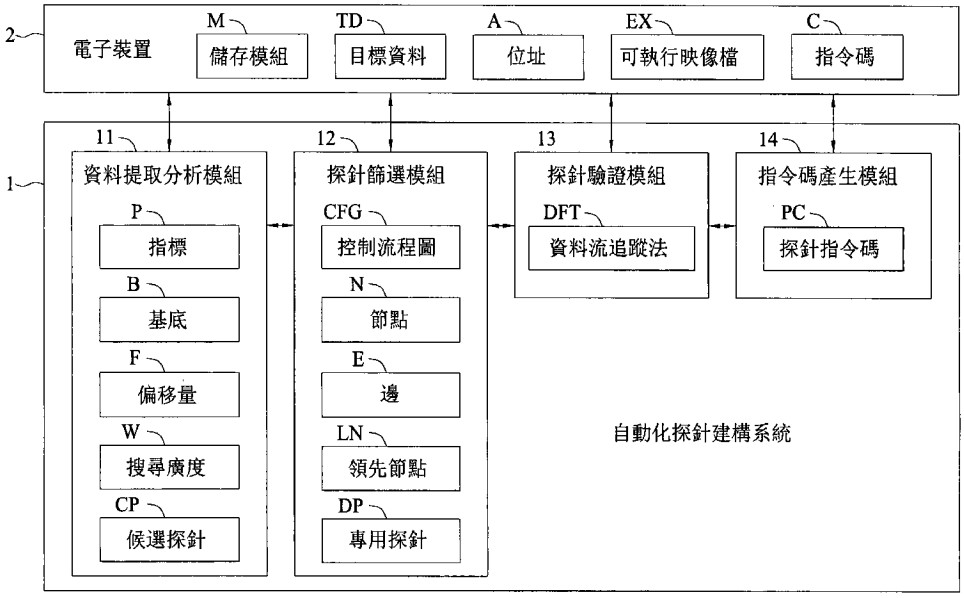
(57)摘要

一種自動化探針建構系統及其方法，該系統包括資料提取分析模組、探針篩選模組與探針驗證模組。該資料提取分析模組係依據複數指標提取電子裝置之複數目標資料及建構複數候選探針。該探針篩選模組係依據該些候選探針與可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一專用探針。該探針驗證模組係自該可執行映像檔中找出對應於該專用探針之指令碼以驗證該專用探針。藉此，本發明可自動建構專用探針並限縮該專用探針之數量。

An automatic probe construction system and method thereof are provided. The system comprises a data dereference analysis module, a probe selection module and a probe verification module. The data dereference analysis module dereferences a plurality of target data of an electronic apparatus and constructs a plurality of candidate probes based on a plurality of pointers. The probe selection module constructs a control flow graph based on the candidate probes and codes of an executable image file to select at least one dedicated probe from the candidate probes by the control flow graph. The probe verification module finds out codes corresponding to the dedicated probe from the executable image file to verify the dedicated probe. Thereby, the invention can automatically construct the dedicated probe and restrict amount of the dedicated probe.

指定代表圖：

TW 201712545 A



第1圖

符號簡單說明：

1・・・自動化探針建構系統

11・・・資料提取分析模組

12・・・探針篩選模組

13・・・探針驗證模組

14・・・指令碼產生模組

2・・・電子裝置

A・・・位址

B・・・基底

C・・・指令碼

CFG・・・控制流程圖

CP・・・候選探針

DFT・・・資料流追蹤法

DP・・・專用探針

E・・・邊

EX・・・可執行映像檔

F・・・偏移量

LN・・・領先節點

M・・・儲存模組

N・・・節點

P・・・指標

PC・・・探針指令碼

TD・・・目標資料

W・・・搜尋廣度

201712545

發明摘要

※申請案號：104134140

※申請日：104. 9. 23　　※IPC分類：

G06F 11/30 (2006.01)

G06F 11/36 (2006.01)

【發明名稱】(中文/英文)

自動化探針建構系統及其方法

AUTOMATIC PROBE CONSTRUCTION SYSTEM AND METHOD THEREOF

【中文】

一種自動化探針建構系統及其方法，該系統包括資料提取分析模組、探針篩選模組與探針驗證模組。該資料提取分析模組係依據複數指標提取電子裝置之複數目標資料及建構複數候選探針。該探針篩選模組係依據該些候選探針與可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一專用探針。該探針驗證模組係自該可執行映像檔中找出對應於該專用探針之指令碼以驗證該專用探針。藉此，本發明可自動建構專用探針並限縮該專用探針之數量。

【英文】

An automatic probe construction system and method thereof are provided. The system comprises a data dereference analysis module, a probe selection module and a probe verification module. The data dereference analysis module dereferences a plurality of target data of an electronic apparatus and constructs a plurality of candidate probes based on a plurality of pointers. The probe selection module constructs a control flow graph based on the candidate probes and codes of an executable image file to select at least one dedicated probe from the candidate probes by the control flow graph. The probe verification module finds out codes corresponding to the dedicated probe from the executable image file to verify the dedicated probe. Thereby, the invention can automatically construct the dedicated probe and restrict amount of the dedicated probe.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

1	自動化探針建構系統	11	資料提取分析模組
12	探針篩選模組	13	探針驗證模組
14	指令碼產生模組	2	電子裝置
A	位址	B	基底
C	指令碼	CFG	控制流程圖
CP	候選探針	DFT	資料流追蹤法
DP	專用探針	E	邊
EX	可執行映像檔	F	偏移量
LN	領先節點	M	儲存模組
N	節點	P	指標
PC	探針指令碼	TD	目標資料
W	搜尋廣度		

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

本案無化學式。

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】（中文/英文）

自動化探針建構系統及其方法

AUTOMATIC PROBE CONSTRUCTION SYSTEM AND METHOD THEREOF

【技術領域】

本發明係關於一種探針建構技術，特別是指一種自動化探針建構系統及其方法。

【先前技術】

資訊安全為每個企業或組織中最不可或缺的需求，故不論產業或學界均致力於更深入的惡意程式之分析技巧。

又，雖然透過探針機制進行作業系統之行為監控或側錄是常見的需求功能之一，但現有探針之實作大多仰賴人工對該作業系統進行逆向工程之分析方能實現。再者，面對未公開原始碼之作業系統，例如微軟作業系統，亦需要人員預先對未公開之核心資料結構進行逆向工程，方能實作對應於該核心資料結構之探針。

但如此一來，因上述逆向工程大多仰賴人工，且該逆向工程之結果缺乏重用性，故當該作業系統之環境變更或版本更新時，將可能迫使人員重複該逆向工程之作業，導致浪費許多的人力成本及時間資源。

因此，如何克服上述先前技術之問題，實已成為目前亟欲解決的課題。

【發明內容】

本發明係提供一種自動化探針建構系統及其方法，其可自動建構專用探針並限縮該專用探針之數量。

本發明之自動化探針建構系統包括：資料提取分析模組，係依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針；探針篩選模組，係依據該些候選探針與該電子裝置之可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一用於該特定事件之專用探針；以及探針驗證模組，係自該電子裝置之可執行映像檔中找出對應於該專用探針之指令碼以驗證該專用探針。

本發明之自動化探針建構方法包括：依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針；依據該些候選探針與該電子裝置之可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一用於該特定事件之專用探針；以及自該電子裝置之可執行映像檔中找出對應於該專用探針之指令碼以驗證該專用探針。

各該指標可具有該電子裝置之儲存模組之基底或該基底加上至少一偏移量，以供該資料提取分析模組依據該些指標之基底與偏移量提取該些目標資料及建構該些候選探針。

該資料提取分析模組可判斷該電子裝置之儲存模組之至少一基底是否包括有效之位址，若是，則再確認由該基

底或該基底加上至少一偏移量所構成之指標之資料為該目標資料，以供該資料提取分析模組提取該目標資料及建構該候選探針。

該控制流程圖可由複數節點與複數連接該些節點之邊所構成，且該些節點分別代表該些候選探針與該可執行映像檔之特定事件之指令碼。

該探針篩選模組可自該些候選探針之節點中分析出至少一領先節點，以移除該領先節點及其邊，俾篩選出至少一專用節點作為該專用探針。

該探針驗證模組可透過資料流追蹤法並依據該專用探針之目標資料、指標、基底與偏移量，以自該可執行映像檔中找出對應於該專用探針之指令碼，俾驗證該專用探針。

該自動化探針建構系統可包括指令碼產生模組，其係依據已驗證之該專用探針產生探針指令碼，且該探針指令碼具有該專用探針之指令碼與提取該目標資料之指令碼。

由上述內容可知，本發明之自動化探針建構系統及其方法中，主要係依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針，以自該些候選探針中篩選出至少一專用探針，且自可執行映像檔中找出指令碼以驗證該專用探針。據此，本發明可自動建構專用探針並大幅限縮該專用探針之數量。

同時，本發明之專用探針可供側錄惡意程式於動態執行時期之行為，並具有安裝於如虛擬機器監視器(VMM)之探針指令碼以取得目標資料及作為側錄工具，且該專用探

針之探針指令碼具有隱匿性以避免惡意程式之干擾及破壞。

另外，本發明之自動化探針建構系統及其方法可應用於各大產業中，如電信服務業、雲端服務產業、防毒軟體公司或相關研究單位等，以利其更快速建立資安系統。

【圖式簡單說明】

第 1 圖係繪示本發明之自動化探針建構系統之方塊示意圖；

第 2 圖係繪示本發明之自動化探針建構方法之步驟流程圖；

第 3A 圖係繪示本發明之自動化探針建構系統及其方法中有關自電子裝置之儲存模組中提取目標資料之示意圖；

第 3B 圖係繪示本發明之自動化探針建構系統及其方法中有關在電子裝置(客戶機)與虛擬機器監視器中執行指令碼之示意圖；

第 4 圖係繪示本發明之自動化探針建構系統及其方法中有關建構複數候選探針之步驟流程圖；

第 5A 圖至第 5E 圖係繪示本發明之自動化探針建構系統及其方法中有關自複數候選探針中篩選出至少一專用探針之控制流程圖；

第 6A 圖係繪示本發明之自動化探針建構系統及其方法中有關專用探針之程序名稱抽取之示意圖；

第 6B 圖係繪示本發明之自動化探針建構系統及其方

法中有關透過資料流追蹤法驗證專用探針之示意圖；以及

第 7 圖係繪示本發明之自動化探針建構系統及其方法中有關專用探針之探針指令碼之示意圖。

【實施方式】

以下藉由特定的具體實施例說明本發明之實施方式，熟悉此技藝之人士可由本說明書所揭示之內容輕易地瞭解本發明之其他優點及功效。

須知，本說明書所附圖式所繪示之結構、比例、大小等，均僅用以配合說明書所揭示之內容，以供熟悉此技藝之人士之瞭解與閱讀，並非用以限定本發明可實施之限定條件，故不具技術上之實質意義，任何結構之修飾、比例關係之改變或大小之調整，在不影響本發明所能產生之功效及所能達成之目的下，均應仍落在本發明所揭示之技術內容得能涵蓋之範圍內。

第 1 圖係繪示本發明之自動化探針建構系統 1 之方塊示意圖，第 2 圖係繪示本發明之自動化探針建構方法之步驟流程圖。

如第 1 圖與第 2 圖所示，自動化探針建構系統 1 可安裝於虛擬機器監視器(Virtual Machine Monitor, VMM)、電腦、伺服器或行動裝置等設備中，並包括資料提取分析模組 11、探針篩選模組 12、探針驗證模組 13 與指令碼產生模組 14。

該自動化探針建構系統 1 及其方法可包括：在步驟 S31 中，令該資料提取分析模組 11 依據複數指標(Pointer)P 自

動提取電子裝置 2 之儲存模組 M 之複數目標資料(Target Data)TD 及自動建構複數用於特定事件之候選探針(Candidate Probe)CP。在步驟 S32 中，令該探針篩選模組 12 依據該些候選探針 CP 與該電子裝置 2 之可執行映像檔(Executable image file)EX 之指令碼(Code)C 自動建構一控制流程圖(Control Flow Graph)CFG，以透過該控制流程圖 CFG 自該些候選探針 CP 中自動篩選出至少一用於該特定事件之專用探針(Dedicated Probe)DP。在步驟 S33 中，令該探針驗證模組 13 自該電子裝置 2 之可執行映像檔 EX 中自動找出對應於該專用探針 DP 之指令碼 C 以驗證該專用探針 DP。在步驟 S34 中，令該指令碼產生模組 14 依據已驗證之該專用探針 DP 自動產生探針指令碼 PC，且該探針指令碼 PC 具有該專用探針 DP 之指令碼 C 與提取該目標資料 TD 之指令碼 C。

各該指標 P 可具有該電子裝置 2 之儲存模組 M 之基底 B 或該基底 B 加上至少一偏移量 F，以供該資料提取分析模組 11 依據該些指標 P 之基底 B 與偏移量 F 提取該些目標資料 TD 及建構該些候選探針 CP。

該電子裝置 2 可為客戶機(Guest)、虛擬機器(VM)、電腦、伺服器或行動裝置(如智慧型手機)等，該儲存模組 M 可為記憶體、暫存器或硬碟等，該目標資料 TD 可為用於該特定事件之資料、使用者有興趣之資料或惡意程式之存取資料等，該特定事件可為該可執行映像檔 EX 之程序創建、檔案創建、機碼設定項(Registry)創建、程序終結、檔

案移除或機碼設定項移除等，該可執行映像檔 EX 可為該電子裝置 2 之作業系統(.sys 檔)或可執行檔(.exe 檔)等，但不以此為限。

第 3A 圖係繪示本發明之自動化探針建構系統 1 及其方法中有關自電子裝置 2 之儲存模組 M 中提取目標資料 TD 之示意圖，第 3B 圖係繪示本發明之自動化探針建構系統 1 及其方法中有關在電子裝置 2(如客戶機 GU)與虛擬機器監視器 VMM 中執行指令碼 C 之示意圖。

如第 3A 圖與上述第 1 圖所示，自該電子裝置 2 之儲存模組 M 中提取該目標資料 TD 之程序可例如為：令該資料提取分析模組 11 以儲存模組 M(如暫存器)之 ESP 為基底 B，並以該基底 B 加上至少一偏移量 F 作為指標 P，再依據該指標 P 自該電子裝置 2 之儲存模組 M 中提取該目標資料 TD。在第 3A 圖中，該至少一偏移量 F 包括三個分別位於堆疊(Stack)ST、NDIS_PACKET 與 NDIS_BUFFER 中之偏移量 F1、F2 及 F3。

如第 3B 圖與上述第 1 圖所示，在該電子裝置 2(如客戶機 GU)與虛擬機器監視器 VMM 中執行指令碼 C 之程序可例如為：當該客戶機 GU 之可執行映像檔 EX(如 NDIS.SYS)執行至指令碼 C「call dword ptr [eax+30h]」時，令該可執行映像檔 EX 暫停執行該指令碼 C 下方之指令碼，且該指令碼 C 會觸發該虛擬機器監視器 VMM 以執行專用探針 DP 之探針指令碼 PC，而當執行完成該探針指令碼 PC 後，令該可執行映像檔 EX 恢復執行該指令碼 C 下方之指令碼。

在本實施例中，第 3B 圖之探針指令碼 PC 係為第 3A 圖中提取目標資料 TD 之指令碼 C，且第 3B 圖之基底 ESP 之指令碼、偏移量 F1-F3 之指令碼與目標資料 TD 之位址 A 之指令碼分別對應於第 3A 圖之基底 ESP、偏移量 F1-F3 與目標資料 TD 之位址 A。

第 4 圖係繪示本發明之自動化探針建構系統 1 及其方法中有關建構複數候選探針 CP 之步驟流程圖。

如第 4 圖與上述第 1 圖所示，建構該候選探針 CP 之程序可例如為：令該資料提取分析模組 11 判斷該電子裝置 2 之儲存模組 M 之至少一基底 B 是否包括有效之位址 A；若是，則令該資料提取分析模組 11 再確認由該基底 B 或該基底 B 加上至少一偏移量 F 所構成之指標 P 之資料為該目標資料 TD，以供該資料提取分析模組 11 提取該目標資料 TD 及建構該候選探針 CP。

詳言之，在第 4 圖之實施例中，可先取得該電子裝置 2 之儲存模組 M 之複數基底 B(如 EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI)。同時，在步驟 S41 中，令該資料提取分析模組 11 逐一判斷各該基底 B 是否包括有效之位址 A；若是，則依據搜尋廣度 W(W1)並以各該基底 B 或各該基底 B 加上預設倍數(如 4 倍數)之偏移量 F1 作為複數指標 P1。

在步驟 S42 中，令該資料提取分析模組 11 逐一判斷各該指標 P1 之資料是否為目標資料 TD。若是(目標資料 TD)，則令該資料提取分析模組 11 執行資料提取程序 DD1(如(EAX, <0>))，藉此提取該電子裝置 2 之儲存模組 M

之目標資料 TD，並建構至少一用於特定事件之候選探針 CP1(如 0x400100→(EAX, <0>))，其中該候選探針 CP1 具有位址 A(如 0x400100)、基底 B(如 EAX)與偏移量 F(如<0>)。反之，若否(非目標資料 TD)，則在步驟 S43 中，令該資料提取分析模組 11 逐一判斷各該指標 P1 之資料是否爲有效位址 A 之指標 P；若是(指標 P)，則依據搜尋廣度 W(W2)並以各該指標 P1 加上預設倍數(如 4 倍數)之偏移量 F2 作爲複數指標 P2。

在步驟 S44 中，令該資料提取分析模組 11 逐一判斷各該指標 P2 之資料是否爲該目標資料 TD。若是(目標資料 TD)，則令該資料提取分析模組 11 執行資料提取程序 DD2(如(EAX, <+4, +4>))，藉此提取該電子裝置 2 之儲存模組 M 之目標資料 TD，並建構至少一用於該特定事件之候選探針 CP2(如 0x400100→(EAX, <+4, +4>))，其中該候選探針 CP2 具有位址 A(如 0x400100)、基底 B(如 EAX)與偏移量 F(如<+4, +4>)。反之，若否(非目標資料 TD)，則在步驟 S45 中，令該資料提取分析模組 11 逐一判斷各該指標 P2 之資料是否爲有效位址 A 之指標 P；若是(指標 P)，則依據搜尋廣度 W(W3)並以該指標 P2 加上預設倍數(如 4 倍數)之偏移量 F3 作爲複數指標 P3。

在步驟 S46 中，令該資料提取分析模組 11 逐一判斷各該指標 P3 之資料是否爲該目標資料 TD。若是(目標資料 TD)，則令該資料提取分析模組 11 執行資料提取程序 DD3(如(EAX, <+4, +4, +12>))，藉此提取該電子裝置 2 之儲

存模組 M 之目標資料 TD，並建構至少一用於該特定事件之候選探針 CP3(如 0x400100→(EAX, <+4, +4, +12>))，其中該候選探針 CP3 具有位址 A(如 0x400100)、基底 B(如 EAX)與偏移量 F(如<+4, +4, +12>)。

第 5A 圖至第 5E 圖係繪示本發明之自動化探針建構系統 1 及其方法中有關自複數候選探針 CP 中篩選出至少一專用探針 DP 之控制流程圖 CFG。

如第 5A 圖至第 5E 圖與上述第 1 圖所示，該探針篩選模組 12 係自該些候選探針 CP 之節點 N 中分析出至少一領先節點 LN，以移除該領先節點 LN 及其邊 E，俾篩選出至少一專用節點作爲該專用探針 DP。

詳言之，在第 5A 圖中，先令該探針篩選模組 12 依據複數節點 N(如 N1-N8)與複數連接該些節點 N(如 N1-N8)之邊 E(如 E1-E8)建構一控制流程圖 CFG，其中該些節點 N(如 N1-N8)分別代表該些候選探針 CP 與該可執行映像檔 EX 之特定事件之指令碼 C。

在第 5B 圖中，令該探針篩選模組 12 自該些節點 N(如 N1-N8)中分析出該些候選探針 CP 之節點 N(如 N4-N8)。

在第 5C 圖中，令該探針篩選模組 12 自該些候選探針 CP 之節點 N(如 N4-N8)中分析出至少一領先節點 LN(如 N4, N7)。

在第 5D 圖與第 5E 圖中，令該探針篩選模組 12 移除該領先節點 LN(如 N4, N7)及其邊 E(如 E4, E7, E8)，藉此篩選出至少一專用節點(如 N8)作爲該專用探針 DP。

第 6A 圖係繪示本發明之自動化探針建構系統 1 及其方法中有關專用探針 DP 之程序名稱抽取(Process Name Extraction)PNE 之示意圖，第 6B 圖係繪示本發明之自動化探針建構系統 1 及其方法中有關透過資料流追蹤法(Data Flow Trace method)DFT 驗證專用探針 DP 之示意圖。

如第 6A 圖與上述第 1 圖所示，有關該專用探針 DP 之程序名稱抽取 PNE 之方式可例如為：(1)以程序名稱 PN「EPROCESS」為基底 B，並以該基底 B 加上偏移量 F1「+312」作為程序名稱 PN「_SECTION_OBJECT」之指標 P1；(2)以該程序名稱 PN「_SECTION_OBJECT」之指標 P1 加上偏移量 F2「+20」作為程序名稱 PN「_SEGMENT」之指標 P2；(3)以該程序名稱 PN「_SEGMENT」之指標 P2 加上偏移量 F3「+0」作為程序名稱 PN「_CONTROL_AREA」之指標 P3；(4)以該程序名稱 PN「_CONTROL_AREA」之指標 P3 加上偏移量 F4「+36」作為程序名稱 PN「_FILE_OBJECT」之指標 P4；(5)以該程序名稱 PN「_FILE_OBJECT」之指標 P4 加上偏移量 F5「+52」作為程序名稱 PN「_UNICODE_STRING」之指標 P5；(6)以該程序名稱 PN「_UNICODE_STRING」之指標 P5 加上偏移量 F6「+0」提取該電子裝置 2 之儲存模組 M 之目標資料 TD。

如第 6B 圖與上述第 1 圖所示，有關透過資料流追蹤法 DFT 驗證專用探針 DP 之方式可例如為：令該探針驗證模組 13 透過該資料流追蹤法 DFT 並依據該專用探針 DP 之目標資料 TD、位址 A、指標 P、基底 B 與偏移量 F，以自

該可執行映像檔EX中找出對應於該專用探針DP之指令碼C以驗證該專用探針DP。

簡言之，從第6B圖右下「開始(Start)」，先自該可執行映像檔EX之指令碼「repz movs [edi], [esi]」之位址[edi]中提取如上述第6A圖之目標資料TD，並透過資料流追蹤法DFT與追蹤方向(見虛線箭頭-->及實線箭頭→)，自該可執行映像檔EX中依序找出或反向推出複數指令碼C，且該些指令碼C係對應於該專用探針DP之位址A、第6A圖之程序名稱PN、偏移量F6-F1、指標P5-P1，藉此驗證該專用探針DP之有效性或實用性。要說明的是，本發明之第6B圖僅顯示與第6A圖相對應之偏移量F6-F2及部分指令碼，而未顯示與第6A圖相對應之程序名稱PN、偏移量F1及指標P5-P1，且第6A圖與第6B圖均未顯示該專用探針DP之位址A。

第7圖係繪示本發明之自動化探針建構系統1及其方法中有關專用探針DP之探針指令碼PC之示意圖。

如第7圖與上述第1圖所示，有關專用探針DP之探針指令碼PC之建構方式可例如爲：令該指令碼產生模組14依據已驗證之專用探針DP產生探針指令碼PC。在第7圖中，該探針指令碼PC之第1-7行係爲該專用探針DP之指令碼C1，而第9-15行係爲提取該目標資料TD之指令碼C2。該探針指令碼PC可安裝於如QEMU或Xen等虛擬機器監視器VMM中，但不以此爲限。

由上述內容可知，本發明之自動化探針建構系統及其

方法中，主要係依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針，以自該些候選探針中篩選出至少一專用探針，且自可執行映像檔中找出指令碼以驗證該專用探針。據此，本發明可自動建構專用探針並大幅限縮該專用探針之數量。

同時，本發明之專用探針可供側錄惡意程式於動態執行時期之行為，並具有安裝於如虛擬機器監視器(VMM)之探針指令碼以取得目標資料及作為側錄工具，且該專用探針之探針指令碼具有隱匿性以避免惡意程式之干擾及破壞。

另外，本發明之自動化探針建構系統及其方法可應用於各大產業中，如電信服務業、雲端服務產業、防毒軟體公司或相關研究單位等，以利其更快速建立資安系統。

上述實施例僅例示性說明本發明之原理、特點及其功效，並非用以限制本發明之可實施範疇，任何熟習此項技藝之人士均可在不違背本發明之精神及範疇下，對上述實施例進行修飾與改變。任何運用本發明所揭示內容而完成之等效改變及修飾，均應為本發明之申請專利範圍所涵蓋。因此，本發明之權利保護範圍，應如申請專利範圍所列。

【符號說明】

1	自動化探針建構系統
11	資料提取分析模組
12	探針篩選模組

13	探針驗證模組
14	指令碼產生模組
2	電子裝置
A	位址
B、ESP	基底
C、C1、C2	指令碼
CFG	控制流程圖
CP、CP1、CP2、CP3	候選探針
DD1、DD2、DD3	資料提取程序
DFT	資料流追蹤法
DP	專用探針
E、E1 至 E8	邊
EX	可執行映像檔
F、F1 至 F6	偏移量
GU	客戶機
LN	領先節點
M	儲存模組
N、N1 至 N8	節點
P、P1 至 P5	指標
PC	探針指令碼
PN	程序名稱
PNE	程序名稱抽取
S31 至 S34、S41 至 S46	步驟
ST	堆疊

TD	目標資料
VMM	虛擬機器監視器
W、W1、W2、W3	搜尋廣度

申請專利範圍

1. 一種自動化探針建構系統，其包括：

資料提取分析模組，係依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針；

探針篩選模組，係依據該些候選探針與該電子裝置之可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一用於該特定事件之專用探針；以及

探針驗證模組，係自該電子裝置之可執行映像檔中找出對應於該專用探針之指令碼以驗證該專用探針。

2. 如申請專利範圍第 1 項所述之自動化探針建構系統，其中，各該指標係具有該電子裝置之儲存模組之基底或該基底加上至少一偏移量，以供該資料提取分析模組依據該些指標之基底與偏移量提取該些目標資料及建構該些候選探針。

3. 如申請專利範圍第 1 項所述之自動化探針建構系統，其中，該資料提取分析模組係判斷該電子裝置之儲存模組之至少一基底是否包括有效之位址，若是，則再確認由該基底或該基底加上至少一偏移量所構成之指標之資料為該目標資料，以供該資料提取分析模組提取該目標資料及建構該候選探針。

4. 如申請專利範圍第 1 項所述之自動化探針建構系統，

其中，該控制流程圖係由複數節點與複數連接該些節點之邊所構成，且該些節點分別代表該些候選探針與該可執行映像檔之特定事件之指令碼。

5. 如申請專利範圍第 4 項所述之自動化探針建構系統，其中，該探針篩選模組係自該些候選探針之節點中分析出至少一領先節點，以移除該領先節點及其邊，俾篩選出至少一專用節點作為該專用探針。

6. 如申請專利範圍第 1 項所述之自動化探針建構系統，其中，該探針驗證模組係透過資料流追蹤法並依據該專用探針之目標資料、指標、基底與偏移量，以自該可執行映像檔中找出對應於該專用探針之指令碼，俾驗證該專用探針。

7. 如申請專利範圍第 1 項所述之自動化探針建構系統，更包括指令碼產生模組，其係依據已驗證之該專用探針產生探針指令碼，且該探針指令碼具有該專用探針之指令碼與提取該目標資料之指令碼。

8. 一種自動化探針建構方法，其包括下列步驟：

依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針；

依據該些候選探針與該電子裝置之可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一用於該特定事件之專用探針；以及

自該電子裝置之可執行映像檔中找出對應於該專

用探針之指令碼以驗證該專用探針。

9. 如申請專利範圍第 8 項所述之自動化探針建構方法，其中，各該指標係具有該電子裝置之儲存模組之基底或該基底加上至少一偏移量，以供該資料提取分析模組依據該些指標之基底與偏移量提取該些目標資料及建構該些候選探針。

10. 如申請專利範圍第 8 項所述之自動化探針建構方法，更包括判斷該電子裝置之儲存模組之至少一基底是否包括有效之位址，若是，則再確認由該基底或該基底加上至少一偏移量所構成之指標之資料為該目標資料，以供該資料提取分析模組提取該目標資料及建構該候選探針。

11. 如申請專利範圍第 8 項所述之自動化探針建構方法，其中，該控制流程圖係由複數節點與複數連接該些節點之邊所構成，且該些節點分別代表該些候選探針與該可執行映像檔之特定事件之指令碼。

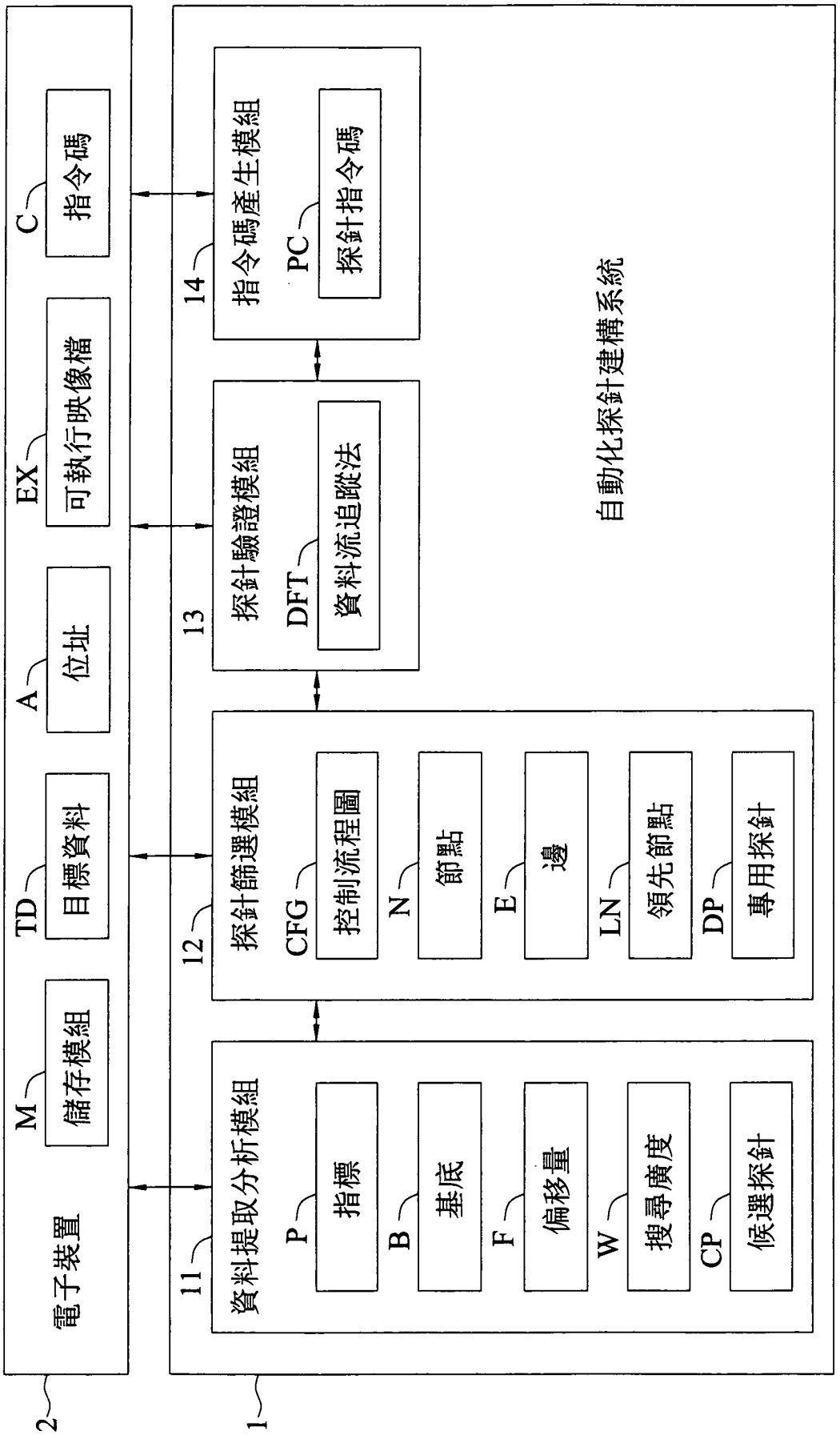
12. 如申請專利範圍第 11 項所述之自動化探針建構方法，更包括自該些候選探針之節點中分析出至少一領先節點，以移除該領先節點及其邊，俾篩選出至少一專用節點作為該專用探針。

13. 如申請專利範圍第 8 項所述之自動化探針建構方法，其中，該探針驗證模組係透過資料流追蹤法並依據該專用探針之目標資料、指標、基底與偏移量，以自該可執行映像檔中找出對應於該專用探針之指令碼，俾

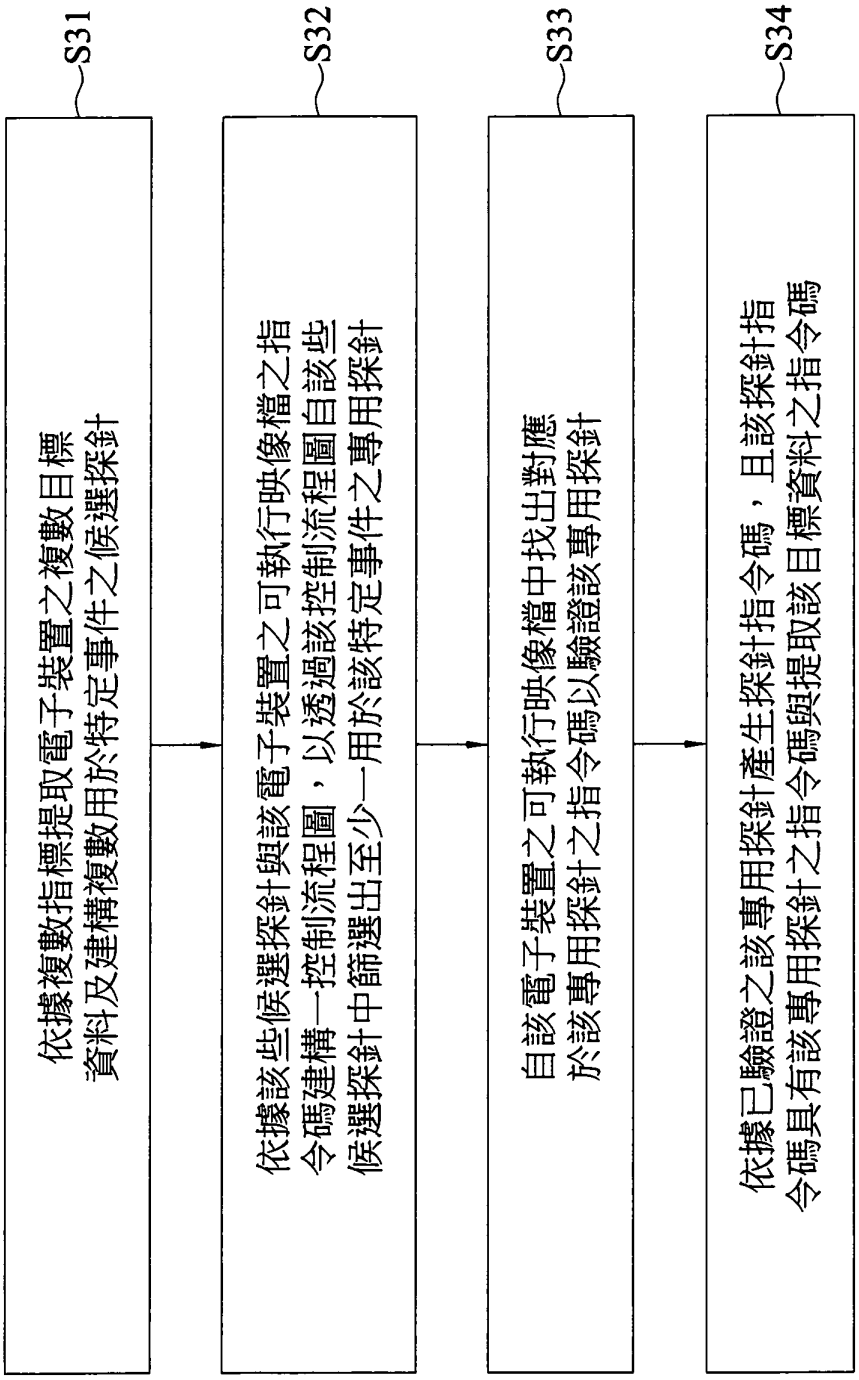
驗證該專用探針。

14. 如申請專利範圍第 8 項所述之自動化探針建構方法，更包括依據已驗證之該專用探針產生探針指令碼，且該探針指令碼具有該專用探針之指令碼與提取該目標資料之指令碼。

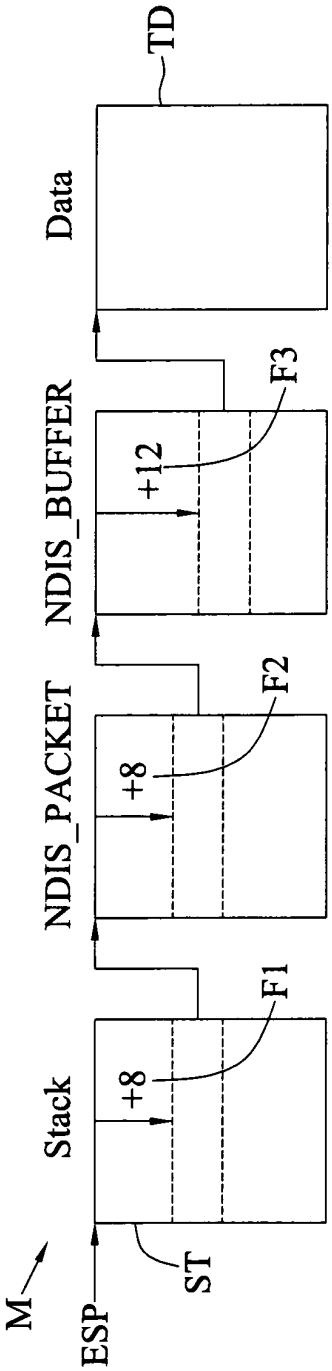
圖式


2
電子裝置
M
儲存模組
TD
目標資料
A
位址
EX
可執行映像檔
C
指令碼
1
自動化探針建構系統
11
資料提取分析模組
P
指標
B
基底
F
偏移量
W
搜尋廣度
CP
候選探針
12
探針篩選模組
CFG
控制流程圖
N
節點
E
邊
LN
領先節點
DP
專用探針
13
探針驗證模組
DFT
資料流追蹤法
14
指令碼產生模組
PC
探針指令碼

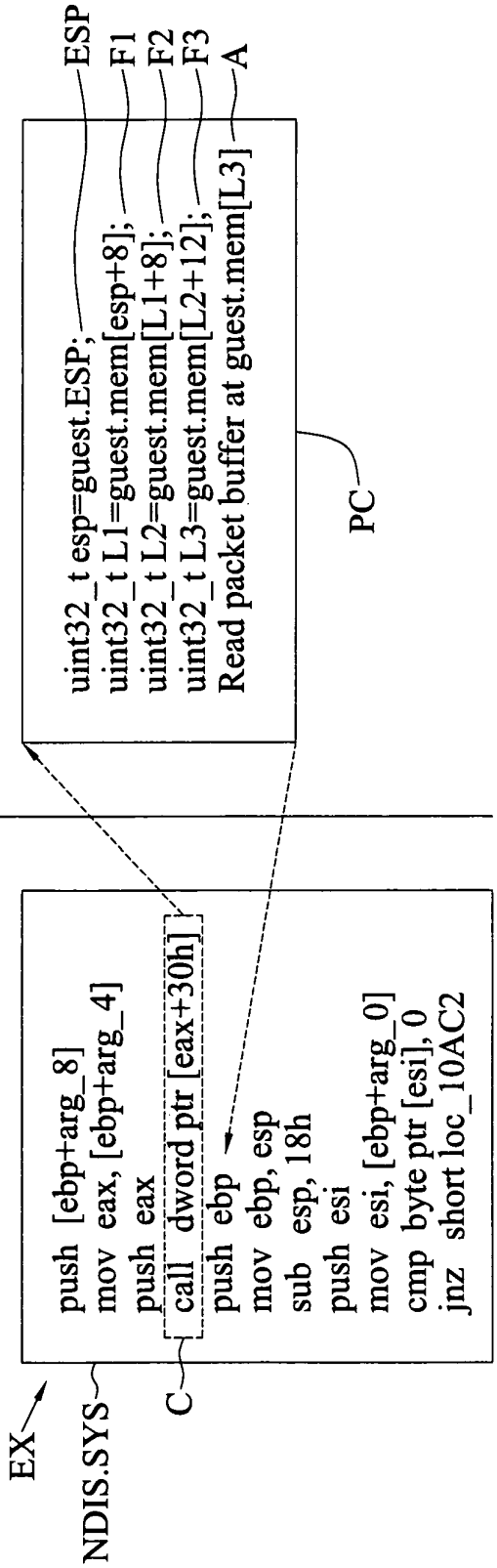
第1圖


S31
依據複數指標提取電子裝置之複數目標資料及建構複數用於特定事件之候選探針
S32
依據該些候選探針與該電子裝置之可執行映像檔之指令碼建構一控制流程圖，以透過該控制流程圖自該些候選探針中篩選出至少一用於該特定事件之專用探針
S33
自該電子裝置之可執行映像檔中找出對應於該專用探針之指令碼以驗證該專用探針
S34
依據已驗證之該專用探針產生探針指令碼，且該探針指令碼具有該專用探針之指令碼與提取該目標資料之指令碼

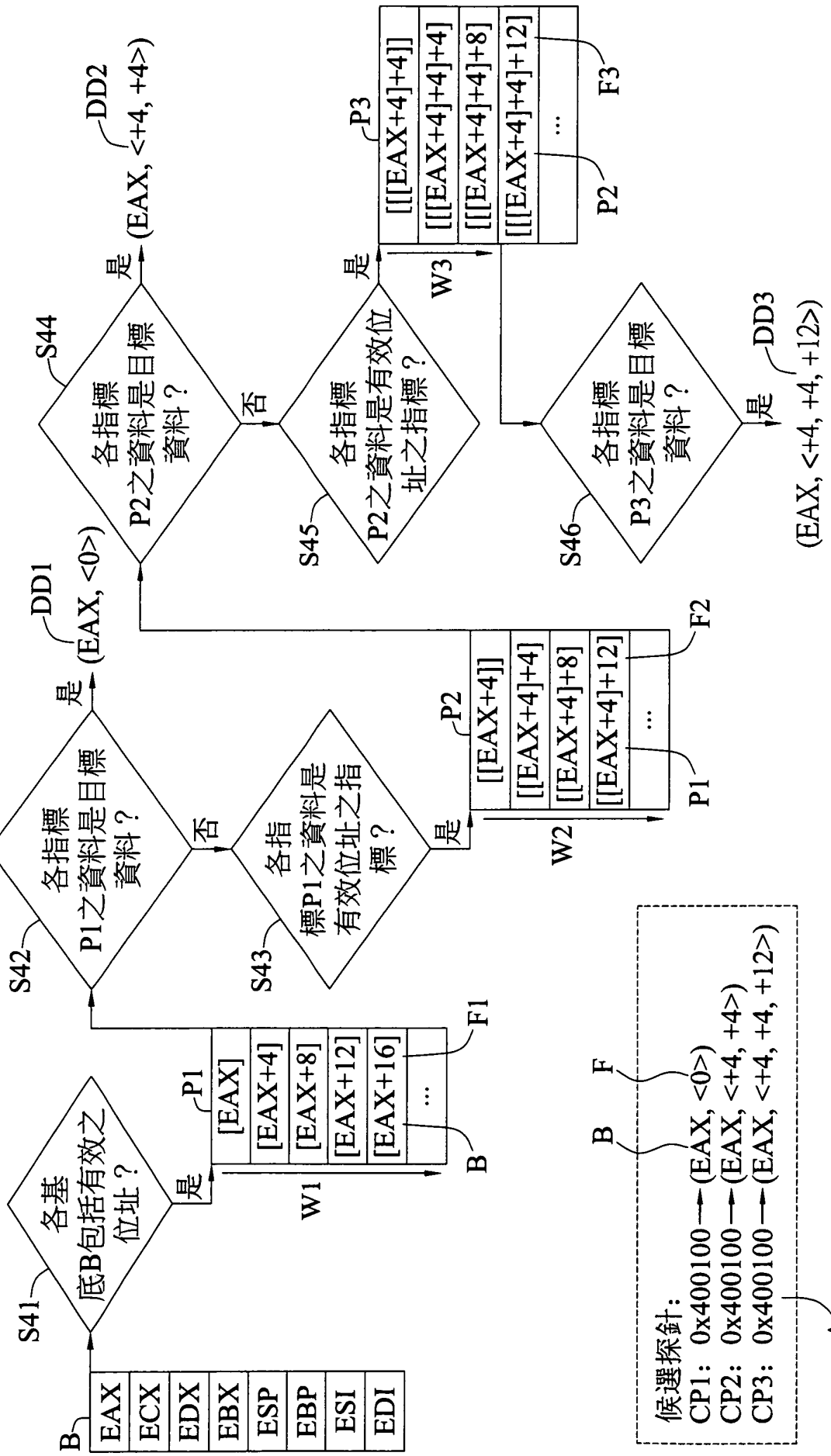
第2圖


M
ESP
ST
Stack
+8
F1
NDIS_PACKET
+8
F2
NDIS_BUFFER
+12
F3
Data
TD

第3A圖


VMM
uint32_t esp=guest.ESP;
uint32_t L1=guest.mem[esp+8];
uint32_t L2=guest.mem[L1+8];
uint32_t L3=guest.mem[L2+12];
Read packet buffer at guest.mem[L3]
ESP
F1
F2
F3
A
PC
GU
push [ebp+arg_8]
mov eax, [ebp+arg_4]
push eax
call dword ptr [eax+30h]
push ebp
mov ebp, esp
sub esp, 18h
push esi
mov esi, [ebp+arg_0]
cmp byte ptr [esi], 0
jnz short loc_10AC2
EX
NDIS.SYS
C

第3B圖


B
EAX
ECX
EDX
EBX
ESP
EBP
ESI
EDI
S41
各基底B包括有效之位址？
是
P1
[EAX]
[EAX+4]
[EAX+8]
[EAX+12]
[EAX+16]
F1
B
W1
S42
各指標P1之資料是目標資料？
是
DD1
(EAX, <0>)
否
S43
各指標P1之資料是有效位址之指標？
是
P2
[[EAX+4]]
[[EAX+4]+4]
[[EAX+4]+8]
[[EAX+4]+12]
F2
P1
W2
S44
各指標P2之資料是目標資料？
是
DD2
(EAX, <+4, +4>)
否
S45
各指標P2之資料是有效位址之指標？
是
P3
[[[EAX+4]+4]]
[[[EAX+4]+4]+4]
[[[EAX+4]+4]+8]
[[[EAX+4]+4]+12]
F3
P2
W3
S46
各指標P3之資料是目標資料？
是
DD3
(EAX, <+4, +4, +12>)
候選探針:
CP1: 0x400100→(EAX, <0>)
CP2: 0x400100→(EAX, <+4, +4>)
CP3: 0x400100→(EAX, <+4, +4, +12>)
A
B
F

第4圖

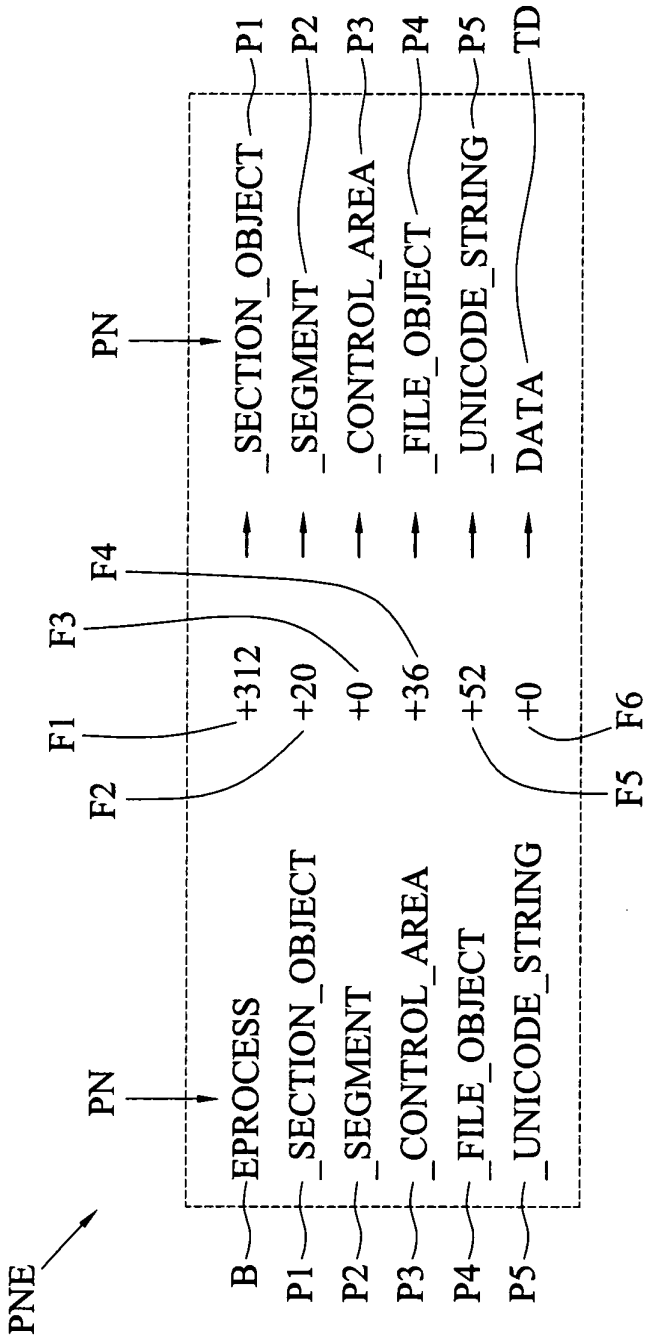
第5A圖

第5B圖

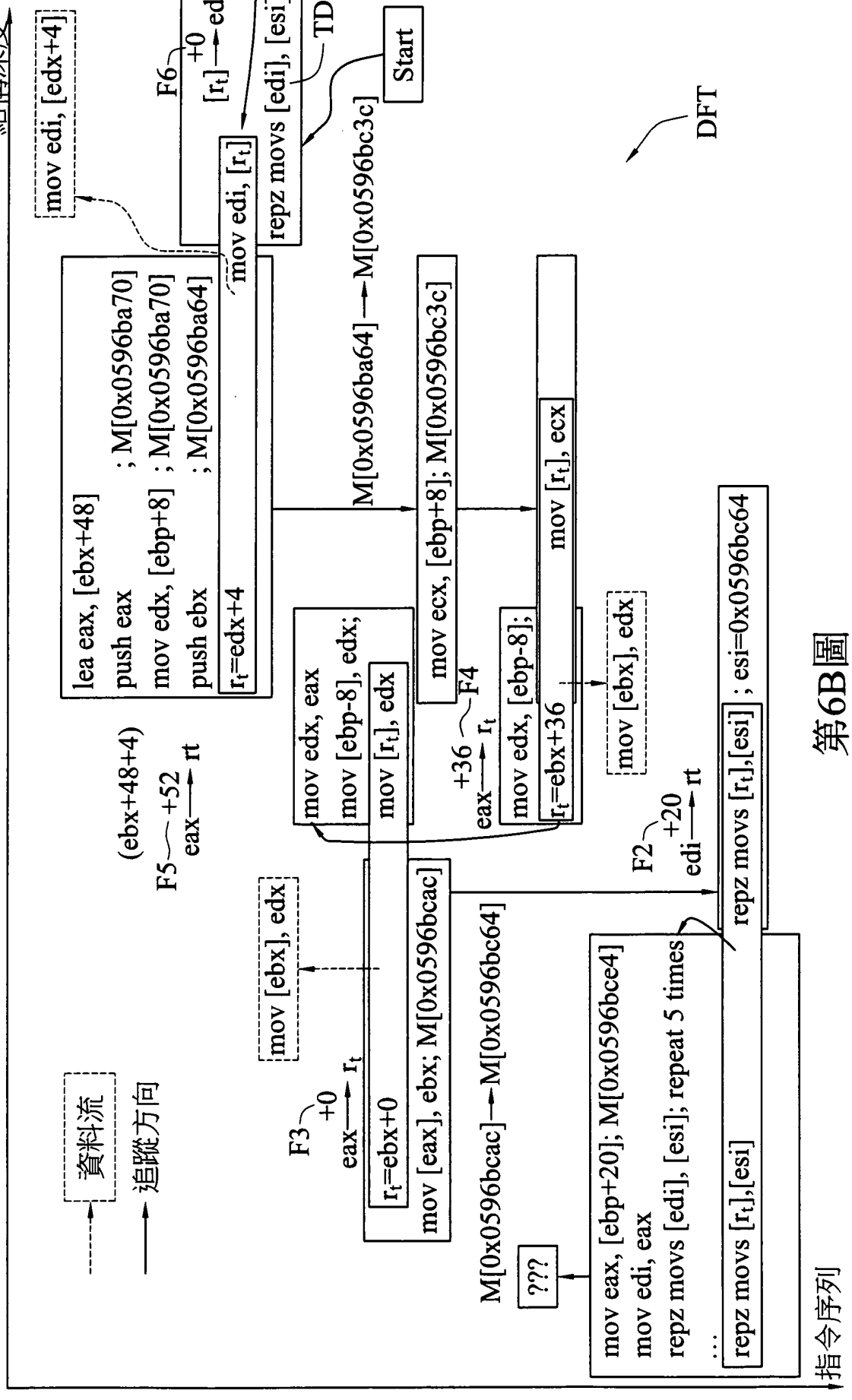
第5C圖

第5D圖

第5E圖


PNE
PN
EPROCESS
_SECTION_OBJECT
_SEGMENT
_CONTROL_AREA
_FILE_OBJECT
_UNICODE_STRING
B
P1
P2
P3
P4
P5
F1
F2
F3
F4
F5
F6
+312
+20
+0
+36
+52
+0
PN
_SECTION_OBJECT
_SEGMENT
_CONTROL_AREA
_FILE_OBJECT
_UNICODE_STRING
DATA
P1
P2
P3
P4
P5
TD

第6A圖


結構深度
指令序列
DFT
資料流
追蹤方向
mov edi, [edx+4]
lea eax, [ebx+48]
push eax ; M[0x0596ba70]
mov edx, [ebp+8] ; M[0x0596ba70]
push ebx ; M[0x0596ba64]
rf=edx+4
mov edi, [rt]
F6
+0
[rt]→edi
repz movs [edi], [esi]
TD
Start
M[0x0596ba64]→M[0x0596bc3c]
mov edx, eax
mov [ebp-8], edx;
mov [rt], edx
mov ecx, [ebp+8]; M[0x0596bc3c]
F4
+36
eax→rt
mov edx, [ebp-8];
rf=ebx+36
mov [rt], ecx
mov [ebx], edx
(ebx+48+4)
F5
+52
eax→rt
mov [ebx], edx
F3
+0
eax→rt
rf=ebx+0
mov [eax], ebx; M[0x0596bcac]
M[0x0596bcac]→M[0x0596bc64]
???
F2
+20
edi→rt
mov eax, [ebp+20]; M[0x0596bce4]
mov edi, eax
repz movs [edi], [esi]; repeat 5 times
...
repz movs [rt],[esi]
repz movs [rt],[esi] ; esi=0x0596bc64

第6B圖

專用探針：0x804e7461(ESP, <+12, +36, +52>)

```
                                                                    PC
1    int gen_probe_804e7461 (unsigned char* buf, size_t len)
2    {
3        int ret = 0;
4        target_ulong ptr = env->regs[R_ESP];
5
6        unsigned int offset[]= {12, 36, 52};
7        unsigned int offsets = 3;
8
9        int i;
10       for (i = 0; i < offsets-1; ++i) {
11           if ((ret=cpu_memory_rw_debug (env, ptr+offset[i], &ptr, sizeof(ptr), 0)) != 0)
12               return ret;
13       }
14       if ((ret=cpu_memory_rw_debug(env, ptr+offset[i], buf, len, 0)) != 0)
15           return ret;
16
17       return 0;
```

C1: lines 4–7

C2: lines 9–15

第7圖