發明專利說明書 200529002

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：94102532

※ 申請日期：2005 年 1 月 27 日　　※IPC 分類：

H06F 15/163

一、發明名稱：（中文/英文）

用於以安全通訊防止電腦裝置在網路環境中產生電腦漏洞之系統與方法

SYSTEM AND METHOD FOR PROTECTING A COMPUTING DEVICE FROM COMPUTER EXPLOITS DELIVERED OVER A NETWORKED ENVIRONMENT IN A SECURED COMMUNICATION

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾苹那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 2 人）

姓　名：（中文/英文）

1.法蘭克亞歷山大/FRANK, ALEXANDER

2.菲利普湯瑪士 G/PHILLIPS, THOMAS. G.

200529002

國　籍：（中文/英文）

1.以色列/Israel

2.美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1.美國；2004 年 2 月 13 日；60/544,772

2.美國；2004 年 6 月 29 日；10/879,837

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明係關於以安全通訊保護計算裝置免於遭受經由網路傳輸的電腦攻擊程式(computer exploit)破壞之系統與方法。

【先前技術】

正當愈來愈多的電腦及其它計算裝置透過各種如網際網路的網路相互連結時，電腦安全已變得愈來愈重要，尤其是經由網路傳輸或透過資訊串流而來的入侵或攻擊。如熟習相關技藝者所知，這類攻擊具有多種形式，其中包括電腦病毒、電腦破壞程式(worm)、系統元件replacement、拒絕服務攻擊，甚至誤用/濫用適格的電腦系統特點，但不以此為限；上述所有攻擊均為不正當的目的而攻擊電腦系統之一個或數個安全性漏洞。雖然熟習相關技藝者當能瞭解，各種電腦攻擊在技術方面各不相同，但為了方便說明本發明之原理，以下將上述各種攻擊統稱為電腦攻擊程式或簡稱為攻擊程式(exploit)。

當某一台電腦受到電腦攻擊程式的攻擊或「感染」到電腦攻擊程式時，會造成各式不同的負面效應，其中包括使系統裝置失效；刪除或竄改韌體、應用程式或檔案資料；將機密資料傳送到網路上的另一個位置；關閉電腦系統；或導致電腦系統當機。儘管不是全部，但大部分的電腦攻擊程式的危害在於受到感染的電腦系統會被用來感染

其它電腦。

第 1 圖係電腦攻擊程式通常進行散佈所透過的網路環境 100 之示意圖。如第 1 圖所示，典型的網路環境 100 包含有數個經由通訊網路 110 相互連結的電腦 102-108；通訊網路 110 可為內部網路或大型通訊網路，例如一般稱作網際網路的廣域 TCP/IP 網路。為了某種原因，某位在連接網路 110 之電腦(例如電腦 102)上的惡意人士開發出一種電腦攻擊程式 112 並將其散佈在網路上。如箭號 114 所示，散佈出來的電腦攻擊程式 112 由一台或數台電腦(例如電腦 104)接收而感染。正如許多電腦攻擊程式的典型情況，一旦受到感染，如箭號 116 所示，電腦 104 將會感染其它電腦(例如電腦 106)，然後如箭號 118 所示再感染別的電腦(例如電腦 108)。顯然地，源於現代電腦網路的速率與影響範圍，使得電腦攻擊程式 112 能以指數型態「成長」，並快速由局部流行而成為全球性的電腦恐慌。

防毒軟體係對抗電腦攻擊程式(特別是電腦病毒和破壞程式)的典型防禦措施。一般而言，防毒軟體會掃瞄經由網路傳送的內送資料，並搜尋與已知電腦攻擊程式有關的可辨識型態。當偵測到與已知電腦攻擊程式有關聯的型態時，防毒軟體的回應可能是移除受到感染資料當中的電腦病毒、隔離資料，或是刪除「受到感染」的內送資料。可惜的是，防毒軟體通常只對「已知」可辨識的電腦攻擊程式有效。此項工作經常是透過將資料當中的型態相配於稱作攻擊程式的「識別特徵(signature)」來完成。此種攻

擊程式偵測模式的其中一個主要缺陷係在於：在電腦的防毒軟體經過更新而能找到新的電腦攻擊程式並對其做出回應之前，未知的電腦攻擊程式可能會在未經檢查的情況下在網路上傳遞。

由於防毒軟體變得更精密而能以更有效率的方式辨認數以千計的已知電腦攻擊程式，電腦攻擊程式亦變得更為複雜難解。舉例而言，目前有許多電腦攻擊程式具有多種型態(polymorphic)；換言之，其不具有現用防毒軟體所認得的可辨識型態或「識別特徵」。由於此類多型態電腦攻擊程式會在傳到另一個電腦系統之前即進行自我修改，使得防毒軟體經常無法辨識它們。

硬體或軟體網路防火牆係另一種目前常見用來防範電腦攻擊程式的措施。熟習相關技藝者當能瞭解，防火牆係一種安全系統，其可藉由控制內部網路與外部網路之間的資訊流通來保護內部網路，以防止外部網路在未經授權的情況下使用內部網路。所有來自於防火牆外部的通訊均會先被送往代理伺服器(proxy)以接受查驗，並判斷該通訊是否安全無虞或容許被轉送到預定到達的目的地。可惜的是，針對一個防火牆進行適當的設定，使其讓容許的網路活動不會受到限制，並拒絕不被容許的網路活動，係一項高度精密且複雜的工作。除技術上的複雜性之外，防火牆的設定亦不易管理。當防火牆未經適當地設定時，容許的網路流通可能會不慎被關閉，而不容許進行的網路流通則可能會被容許通過，因而危及到防火牆的安全性。故此，

一般很少針對防火牆進行變更，而且只有精通網路設計技術者才能執行此項工作。

防火牆的另一項限制在於：正當防火牆在保護內部網路時，其將不會為特定電腦提供保護。換言之，一個防火牆不會使其本身適應於特定電腦的需求。即使利用防火牆來保護單獨一台電腦，其仍將根據該防火牆的設定架構來保護該電腦，而不是根據該單一電腦之設定組態來進行保護。

另一項關於防火牆的問題係在於：防火牆無法提供免於受到源自於其所建立之邊界內部的電腦攻擊程式破壞的保護。換言之，一旦攻擊程式能夠穿過防火牆所保護的網路後，防火牆即無法禁止該攻擊程式。當一位雇員將可攜式電腦帶回家(亦即不受到公司防火牆的保護)，並在較不安全的環境下使用該電腦時，經常會發生上述情況。此可攜式電腦隨後會在該雇員不知情的情況下被感染。當該可攜式電腦重新連上受到防火牆保護的公司網路時，攻擊程式經常會在未經防火牆查驗的情況下任意感染別的電腦。

如前所述，目前的電腦攻擊程式亦能在某一攻擊活動中利用適格的電腦系統特點。除防火牆和防毒軟體提供者之外的許多團體，現在必須加入防範電腦受到電腦攻擊程式破壞的行列。舉例而言，作業系統提供者現在必須為了經濟或合約方面的理由，持續分析其作業系統的功能，以便找出可能會被電腦攻擊程式利用的弱點或安全性漏

洞。為在此討論內容之便，電腦攻擊程式可能會利用來攻擊電腦系統的管道將通稱為電腦系統安全性漏洞，或簡稱為安全性漏洞。

當在作業系統或其它電腦系統元件、驅動程式或應用程式內發現到安全性漏洞時，提供者通常會發佈軟體更新程式來修補該項安全性漏洞。此類通常被稱作修補程式的更新程式應該安裝在電腦系統上，以便使電腦系統免於受到安全性漏洞的威脅。然而，此類更新程式在本質上是程式碼，其可變更作業系統元件、裝置驅動程式或軟體應用程式。就此而言，此類更新程式的發佈無法如同防毒軟體提供者一樣地進行快速且大量的防毒碼更新。由於此類更新係程式碼變更，使得軟體更新在發佈到公眾領域之前，必須先行經過提供者內部的大量測試。可惜的是，即使一項軟體更新會先經過公司內部的測試，其仍可能會導致其它一項或多項電腦系統特點損壞或功能失常。因此，軟體更新會為仰賴電腦系統的當事者造成一種極大的兩難情況。確切而言，當事者應該冒著電腦系統損壞的風險來更新其電腦系統，使其免於受到安全性漏洞的威脅？還是不應該更新其電腦系統而冒著其電腦系統可能會受到感染的風險？

在目前的系統當中，有一段在此稱作安全性漏洞空窗期(vulnerability window)，其存在於新的電腦攻擊程式散佈在網路 110 上與電腦系統經過更新以保護其免於受到該電腦攻擊程式威脅等兩個時間點之間。正如其名稱所暗

示者，電腦系統係在此安全性漏洞空窗期內存在安全性漏洞，或面臨新的電腦攻擊程式之威脅。第 2A 圖和第 2B 圖係時間線範例的方塊圖，其繪示安全性漏洞空窗期。以下關於時間線的說明當中，重要的時間或事件將會被視為並稱作關於時間線的事件。

第 2A 圖繪示電腦系統關於其中一種最新散佈在公共區域網路的先進電腦攻擊程式類別的安全性漏洞空窗期。此種新式的電腦攻擊程式會利用系統提供者的預應式(proactive)安全措施來找出電腦系統的安全性漏洞，然後再建立及散佈電腦攻擊程式；關於此點，以下將會提供進一步的說明。

請參照第 2A 圖；在事件 202 處，作業系統提供者在發行的作業系統當中找到安全性漏洞。舉例而言，在某一種情境下，作業系統提供者針對發行的作業系統執行自身的內部分析時，發現到先前未知並可用來攻擊電腦系統的安全性漏洞。在另一種情境當中，第三人(其中包括針對電腦系統進行系統安全性分析的機構)發現先前未知的安全性漏洞，並將關於此安全性漏洞的資訊轉告作業系統提供者。

一旦作業系統提供者得知存在安全性漏洞，作業系統提供者會在事件 204 處解決此安全性漏洞而導向修補程式的建立和發佈，以保護執行該種作業系統的電腦系統。作業系統提供者通常會發出某種宣告，告知可以取用某種系統修補程式，同時會建議所有的作業系統使用者安裝該

修補程式。此類修補程式通常會存放在網路 110 上的已知位置，以供下載並安裝在受到影響的電腦系統。

可惜的是，在事件 206 處，經常在作業系統提供者發佈修補程式後，惡意的人士會下載該修補程式，並利用某種還原工程(reverse engineering)及任何由作業系統或其它系統所公布的資訊來找出作業系統內「已修補的」安全性漏洞之技術細節。惡意的人士可以利用此資訊來建立能攻擊潛在安全性漏洞的電腦攻擊程式。在事件 208 處，惡意人士將電腦攻擊程式散佈在網路 110 上。雖然發佈軟體修補程式—亦稱作「修補程式」—的目的是要修正潛在的安全性漏洞，但可惜的是：「修補程式」本身經常是一段複雜的軟體程式碼，使其可能會形成或含有新的安全性漏洞，進而可能會遭受到惡意人士所製造的電腦攻擊程式的攻擊。因此，除了要評估「修補程式」到底修正了什麼之外，還需要相對於潛在的安全性漏洞來評估「修補程式」。

儘管可以取得「修補程式」，基於各種包括上述在內的理由，惡意人士能瞭解到並非每一種電腦系統均會立即接受升級。因此，在事件 208 處，惡意人士會將電腦攻擊程式 112 散佈在網路 110 上。如上所述，電腦攻擊程式 112 的散佈會開啟安全性漏洞空窗期 212；其中，存在安全性漏洞的電腦系統會受到此攻擊程式的威脅。在事件 210 處，唯有當修補程式最終安裝在電腦系統上時，該電腦系統上的安全性漏洞空窗期 212 才得以結束。

儘管目前散佈的許多電腦攻擊程式係基於已知的安

全性漏洞—例如第2A圖所繪示的情況，但散佈在網路110上的電腦攻擊程式有時會利用先前未知的安全性漏洞。第2B圖繪示在此種情況下相對於時間線220的VUL空窗期230。因此，如時間線220所示，在事件222處，惡意人士散佈一種新的電腦攻擊程式。由於此為新的電腦攻擊程式，作業系統修補程式與防毒更新程式均無法取得，以使受到安全威脅的電腦系統得免於遭受攻擊。因此之故，VUL空窗期230處於開啟狀態。

如事件224所示，在新的電腦攻擊程式流傳於網路110之後的某個時間點上，作業系統提供者及/或防毒軟體提供者會偵測到此新的電腦攻擊程式。熟習相關技藝者當能瞭解，作業系統提供者和防毒軟體提供者通常會在幾個小時內偵測到新的電腦攻擊程式的出現。

一旦偵測到電腦攻擊程式，防毒軟體提供者即能開始進行辨識模式(pattern)或「識別特徵」的程序；防毒軟體可藉此程序辨識電腦攻擊程式。同樣地，作業系統提供者會開始進行分析電腦攻擊程式的程序，以判斷作業系統是否必須加以修補，以防範受到電腦攻擊程式的攻擊。在事件226處，經過上述類似的努力，作業系統提供者及/或防毒軟體提供者會發佈對付該電腦攻擊程式的更新，亦即作業系統的軟體修補程式或防毒碼更新。接著，在事件228處，此更新會安裝在使用者的電腦系統上，藉以保護電腦系統並結束VUL空窗期230。

由上述實例可知—其僅為電腦攻擊程式對電腦系統

造成安全性威脅之所有可能情況的範例，VUL 空窗期係存在於當電腦攻擊程式 112 散佈在網路 110 上與當對應的更新安裝在使用者之電腦系統上並結束該 VUL 空窗期兩時間點之間。可惜的是，不論 VUL 空窗期長短與否，針對受到感染的電腦進行可能的「解毒」及修復將會耗費電腦擁有者大量的金錢。對處理擁有數千或數十萬台連上網路 110 之裝置的大型公司或機構而言，此成本可能會非常龐大。若電腦攻擊程式已竄改或破壞客戶的資料，而極難或不可能追蹤並加以補救，則此項成本將會更加龐大。吾人需要一種以回應的方式及根據個別電腦系統之需求來保護電腦系統的系統及方法，使其在取得保護更新及/或安裝在電腦系統之前，即能免於受到電腦攻擊程式的威脅。本發明可解決上述及習知技術所遭遇到的其它問題。

【發明內容】

本發明之技術態樣提供一種介於計算裝置與網路之間的網路安全模組，用於保護該計算裝置，使其免於受到在網路上找到的安全威脅。此種網路安全模組的設置方式係使得電腦與網路之間的所有網路活動均會通過該網路安全模組。此網路安全模組包含有計算裝置連線。此計算裝置連線可將上述網路安全模組連接到計算裝置。上述網路安全模組亦包括能使網路安全模組連上網路的網路連線。網路活動係經由計算裝置連線和網路連線而通過網路安全模組。上述網路安全模組亦包括一解碼器模組；該解碼器

模組能利用取得的解密金鑰來針對安全性通訊進行暫時解密。上述網路安全模組另包含一安全執行模組；該安全執行模組能控制計算裝置與網路之間的網路活動。安全執行模組能執行取得的安全措施，藉以保護計算裝置免於受到在網路上找到的安全威脅。

本發明之另一技術態樣提供一種介於計算裝置與網路之間的網路安全模組所執行的方法，該方法能使該計算裝置與該網路之間的網路活動均必須通過該網路安全模組，以保護該計算裝置免於受到安全威脅。如此即可得到預應的(proactive)安全措施。當實行保護安全措施時，其可保護計算裝置免於受到辨識到的安全威脅。送往計算裝置的安全通訊會被偵測到。如此，受到保護的安全通訊即能暫時被解密。隨後，保護安全措施會在暫時解密的安全通訊上執行。

【實施方式】

第 3A 圖為適於實施本發明之技術態樣的網路環境 300 示意圖。示範性網路環境 300 包含有連接到網路 110 的電腦 302。需注意的是：雖然在此係以如電腦 302 的個人電腦之相關操作來概括說明本發明，但目的僅為舉例說明，而不應被解讀成本發明的限制。熟習相關技藝者當能瞭解，幾乎所有的網路化計算裝置均有可能會遭受到電腦攻擊程式的攻擊。因此，實施本發明將有利於保護各式各樣的電腦、計算裝置或電腦系統，其中包括但不限於：個

人電腦、平板型電腦(tablet computers)、筆記型電腦、個人數位助理(PDA)、迷你及大型主機電腦、無線電話/PDA之組合，以及類似裝置。實施本發明亦有利於保護硬體裝置、週邊裝置、軟體應用程式、裝置驅動程式、作業系統，以及類似裝置或程式。

熟習相關技術者需瞭解，網路 110 包括數量不限的實際通訊網路。此類實際通訊網路包括但不限於：網際網路、廣域及區域網路、內部網路、行動網路、IEEE 802.11 和藍芽無線網路，以及類似網路。因此，雖然在此係以電腦網路的角度來說明本發明，其目的僅為舉例說明，而不應被解讀成本發明的限制。

示範性網路環境 300 亦包括網路安全模組 304 及安全服務 306。網路安全模組 304 係介於電腦—例如電腦 302—與網路 110 之間。網路安全模組 304 可以實體或邏輯方式配置在電腦 302 與網路 110 之間。電腦 302 與網路 110 之間的通訊會通過網路安全模組 304。根據本發明，網路安全模組 304 可根據對應於電腦之特定組態的安全性資訊來選擇性地控制電腦 302 與網路 110 之間的網路活動；電腦之特定組態包括但不限於安裝在電腦 302 上的特定作業系統修訂、包含防毒軟體與對應識別特徵資料檔在內的防毒資訊、安裝的應用程式、裝置驅動程式及類似組態，其中上述所有特定組態均有可能是電腦攻擊程式的潛在目標而成為電腦系統漏洞。

根據本發明之一實施例，為了定期從安全服務 306

取得安全性資訊，網路安全模組304會定期向安全服務306提出對應於電腦302之特定組態的安全性資訊的安全性資訊要求。經過設定，網路安全模組304可以定期從安全服務306取得安全性資訊。舉例而言，吾人可以設定網路安全模組304，使其每分鐘從安全服務306取得安全性資訊。或者，吾人可以設定網路安全模組 304，使其根據使用者指定的時間而從安全服務306取得安全性資訊。

由於許多使用者會為了各種原因而必須延遲為其電腦系統進行更新，因此取得對應於電腦之特定組態的安全性資訊顯得非常重要。舉例而言，針對作業系統或防毒軟體進行更新的延遲，可能是因為電腦已有一段時間未使用。因此，雖然最新修訂的作業系統及/或防毒軟體可以提供足夠的保護來防止最新發現的電腦攻擊程式的攻擊，但電腦仍有可能不是「最新的狀態」，因此容易受到電腦攻擊程式的影響而必須採取符合電腦之特定組態的安全措施。有鑑於此，安全性資訊要求可包括但不限於：包含已安裝的修補程式在內的電腦作業系統修訂之識別資訊；電腦所使用的特定防毒軟體和其修訂，以及軟體及資料檔的更新；以及具有網路功能的應用程式資訊，例如電子郵件或瀏覽器識別符、修訂、韌體提供者和版本以及其它安全性設定。

根據本發明之技術態樣，當針對電腦系統元件進行更新時，其中一個動作即是由網路安全模組304取得電腦之特定組態資訊。舉例而言，當使用者將作業系統之修補

程式安裝在電腦 302 上時，其中一個安裝動作即是將目前修訂的作業系統版本告知網路安全模組 304。同樣地，其它如具備網路功能的應用程式或防毒軟體等電腦系統特點亦會在其被安裝時告知網路安全模組 304，使得網路安全模組可以取得最確實及足夠的安全性資訊，以根據電腦目前的特定組態來保護電腦 302。

根據安全性資訊要求當中的電腦特定組態資訊，安全服務 306 可以找到相關的安全資訊，以保護電腦使其避免出現已知或察覺到的電腦系統安全性漏洞。以下將會針對找出相關的安全性資訊方面進行更詳盡的解說。安全性資訊包括由網路安全模組 304 執行的保護安全措施，此保護措施能讓網路安全模組將電腦 302 與已知安全性漏洞之電腦攻擊程式隔離。保護安全措施包括任意數目的網路活動控制或其組合，其中包括但不限於：封鎖電腦 302 與網路 110 之間的所有網路活動，但不包括某些已知的安全網路位置(例如安裝修補程式或更新的安全服務 306 或防毒軟體服務 308)之間的通訊；封鎖在特定通訊埠及位址上的通路；封鎖某些網路相關應用程式—例如電子郵件或網頁瀏覽應用程式—的來往通訊；以及拒絕存取電腦 302 上的特定硬體或軟體元件。以此方式，網路安全模組會在收到安全性回應後執行安全措施。

如上所述，網路安全模組 304 係介於電腦 302 與網路 110 之間；就此而言，電腦與網路之間的所有網路活動均必須通過網路安全模組。當網路傳輸通過網路安全模組

304 時，網路安全模組會監視網路傳輸情況，並執行從安全服務 306 接收而來的保護措施，例如：封鎖所有的網路存取活動，但不包括某些已知為安全位置之間的通訊，或類似安全措施。

根據本發明之另一技術態樣，一項安全回應亦可包含指定的安全性層級，例如紅色、黃色和綠色層級。對電腦 302 的使用者而言，安全性層級係代表由網路安全模組 304 所執行的保護措施之層級。舉例而言，紅色安全性層級可以表示網路安全模組 304 目前正在封鎖電腦 302 與網路 110 之間的所有網路活動，但此封鎖不包括已知為安全位置的存取活動。或者，黃色安全性層級可以表示網路安全模組 304 目前正在執行某些保護安全措施，而電腦 302 仍然可以與網路 110 聯繫。此外，綠色安全性層級可以表示網路安全模組 304 未執行任何一種保護安全措施，且電腦 302 與網路 110 之間的通訊未受到限制。根據上述安全性層級，為便於說明起見，紅色安全性層級亦可稱作完全封鎖，黃色安全性層級亦可稱作部分封鎖，綠色安全性層級則可稱作自由網路存取。雖然以上提到三種安全性層級以及紅色、黃色和綠色等表示法，但其僅為舉例說明，而不應被解讀為本發明之限制。熟習相關技藝者當能瞭解，吾人可以實施任意數目的安全性層級，並可為使用者提供別種表示法。

由於網路安全模組 304 係以自動化方式運作，亦即不需要使用者的介入，因此上述安全性層級以及任何一種

對應的安全性層級表示法之目的僅為提供使用者資訊而已，並可為使用者指出網路安全模組 304 所執行的限制層級。當使用者試圖判斷網路連線是否有功能異常的情況時，或判斷是否因考量到目前網路安全性而限制網路活動時，此圖像表示法特別有用。

根據本發明之技術態樣，其增加一種安全性措施，當開啟網路安全模組 304 的電源時，其會進入到預設狀態。此預設狀態相當於最高安全性層級，亦即完全封鎖的狀態，但容許進行電腦 302 與信任的網路位置之間的網路活動。不論是在電源開啟的過程中，或是在定期與安全服務 306 進行聯繫的過程中，網路安全模組 304 均會取得最新的安全性資訊，並可依照此安全性資訊來採取較不嚴格的安全性措施。在網路安全模組 304 上執行預設狀態顯然對電腦 302 非常有利，因為在網路安全模組處於電源關閉期間，可能會出現安全性漏洞，或者攻擊程式已散佈在網路 110 上。

根據本發明之一實施例，網路安全模組 304 不會要求或存取來自於電腦 302 的資訊。網路安全模組 304 反而會在某些事件上針對從電腦 302 傳送而來的資訊進行操作。因此，當網路安全模組 304 首次開始保護電腦時，例如當網路安全模組首次配置在電腦 302 與網路 110 之間時，網路安全模組 304 將不會有任何對應於電腦系統的特定組態資訊。如上所述，當網路安全模組 304 沒有電腦 302 的相關組態資訊時，或當網路安全模組 304 的電源被開啟

時，網路安全模組會進入到其預設狀態，亦即完全封鎖狀態。然而，如上所述，完全封鎖將仍然容許電腦 302 聯繫已知的安全位置。舉例而言，此類已知的安全位置包括作業系統更新程式的一個或數個存放位置。因此，即使電腦 302 設有最新的作業系統、防毒軟體、應用程式以及可用的裝置驅動程式之修訂和更新，使用者仍然可以執行更新程序而產生會被傳送到網路安全模組 304 的組態資訊。在另一種實施方式中，特殊程式可以將電腦系統目前的組態告知網路安全模組 304。

為了確保網路安全模組 304 與安全服務 306 之間的通訊係真實可靠且未被竄改，在本發明之一實施例中，網路安全模組與安全服務之間的通訊—例如安全性要求和安全性資訊—會以加密的安全通訊(例如採用安全套接字層(Secure Sockets Layer, SSL)協定)進行傳送。同樣地，網路安全模組 304 與電腦 302 之間的通訊亦以類似方式加以保護。

根據本發明之非必要性技術態樣，即使當電腦關閉時，網路安全模組 304 仍會持續運作，亦即取得對應於電腦 302 的安全性資訊。舉例而言，當網路安全模組 304 被開啟時，其可完全依照提供給電腦的最新作業系統及/或防毒軟體修訂資料來持續取得用於電腦 302 的安全性資訊。根據一實施例，網路安全模組 304 係連接到電腦的輔助電源軌(power rail)；如熟習相關技藝者所知，輔助電源軌可在電腦 302 處於關閉狀態時提供電源給週邊裝置。此外，

若網路安全模組 304 只在電腦 302 操作期間運作，則當網路安全模組重新運作時，網路安全模組將會執行完全封鎖，同時取得對應於電腦目前組態的最新安全性資訊。

根據本發明之另一實施例，使用者可以選擇停用網路安全模組 304。此項操作非常有用，因為有時能夠完全使用網路的必要性會比承擔電腦攻擊程式之攻擊的風險來得重要。舉例而言，當嘗試針對網路問疑難問題進行偵錯時，可能必須停用網路安全模組 304。或者，某些緊急情況—例如使用 E911 語音網路(VoIP)服務—可能必須要停用網路安全模組 304。

根據本發明之技術態樣，當網路安全模組 304 被停用時，其會持續取得來自於安全服務 306 的安全性資訊，然而其不會執行保護安全措施。由於網路安全模組在重新啟用時將會有最新的安全性資訊，因此對使用者而言，持續針對安全性資訊進行更新非常有利；尤其是在網路安全模組 304 只是暫時被停用的情況。在另一種情況下，若網路安全模組 304 被停用且未持續更新，則網路安全模組會在沒有和安全服務 306 進行任何通訊的一段預設時間之後，重新回復到其預設狀態—即網路活動的完全封鎖。

安全服務 306 的實作方式可為所有安全性資訊的單一伺服器/來源，或者為分散在網路 110 上的伺服器/來源階層架構。在階層化系統當中，網路安全模組 304 會接受安全服務裡的根伺服器/服務必定會進行的初始化設定。然而，或許在網路安全模組 304 與安全服務之間首次進行通

訊時，安全服務會提供安全服務之階層架構的相關資訊，以當作安全服務所傳回的安全性資訊之一部分。此資訊可為一個或數個網路位址的範圍，其均為安全服務階層架構的節點，並能將適當的安全性資訊提供給網路安全模組304。其後，網路安全模組304即不需要查詢原始節點來獲得資訊。顯然地，以階層方式實作安全服務之優點在於：吾人可輕易地放大或縮小安全服務的規模來配合提出資訊要求的網路安全模組數目，使得安全服務階層的原始節點將不會被來自於網路上的所有網路安全模組的安全性資訊要求摧垮。在分散於網路110的階層化結構之下，可以得到負載平衡的效果，且備援結構可內建於系統當中，使得在階層架構內的某一節點失效時，其它節點仍可接管來提供安全性資訊。

根據本發明之技術態樣，利用習知的通訊埠模仿(port mimicking)技術，電腦302和網路110將無法察覺到網路安全模組304的存在。概括而言，利用通訊埠模仿技術，對電腦302來說，網路安全模組304即像是網路110；而對網路上的裝置來說，網路安全模組304即像是電腦。因此，除非網路安全模組認定通訊係導向網路安全模組(例如通知進行作業系統更新或安全性資訊回應)，或者網路安全模組必須根據保護安全措施來封鎖網路活動，否則電腦302與網路110之間透過網路安全模組的網路活動可以自由地流通。

如上所述，經過查詢之後，網路安全模組304可從

安全服務 306 取得安全性資訊。熟習相關技藝者當能瞭解，此係一種輪詢系統(poll system)，亦即為取得安全性資訊而輪詢安全服務 306。然而，在另一種實施例中，安全服務 306 可以較有利的方式將重要的安全性資訊播送到網路 110 當中的網路安全模組。舉例而言，若破壞力特別強的電腦攻擊程式開始在網路 110 上流傳，安全服務會取決於網路環境 300 內的網路安全模組從安全服務 306 取得安全性資訊的時間週期，將安全性資訊播送到網路安全模組，而不會等待網路安全模組要求重要的安全性資訊。此安全性資訊—以下稱作安全性佈告—通常包括容易受到電腦攻擊程式影響的所有組態、將要採取的保護措施，以及標示對應的安全性層級。根據本發明之一實施例，安全性佈告係依照預定設計概要所規劃的 XML 文件。

將資訊播送給聽取者的系統係稱作推送系統，亦即安全服務 306 將重要的安全性資訊推送給網路安全模組。根據本發明之技術態樣，安全性佈告係一種利用「保證傳輸」服務在網路 110 上進行播送的方式。在保證傳輸服務當中，安全性佈告係被視為高優先的項目，並會在網路服務提供者的同意之下，比其它原本要先行傳送的網路流通更先進行傳輸。

除了在電腦 302 連上的同一個網路 110 上傳送安全佈告之外，許多時候在「埠帶外(out-of-band)」進行通訊將會非常有幫助，亦即透過與網路 110 分離的輔助通訊連結來進行通訊。第 3B 圖為另一種網路環境 310 之示意圖，

所示環境適於實施本發明之各式技術態樣，其中包括輔助通訊連結 314，其可用來將安全性資訊傳送到連上網路 110 的網路安全模組。

如第 3B 圖所示，另一種網路化環境 310 包含如網路化環境 300 所示之類似元件，其中包括電腦 302、安全服務 306 和網路安全模組 304。然而，安全服務 306 另外經過設定而能將安全性資訊—包括安全性資訊及/或安全性佈告—傳送到網路安全模組 304；此外，網路安全模組特別配接一個經由輔助通訊連結 314 來接收資訊的接收裝置 312。根據本發明之技術態樣，輔助通訊連結 314 可為衛星通訊連結、無線電頻率播送，或其它設於安全服務 306 與網路安全模組 304 之間的輔助通訊。熟習相關技藝者當能瞭解，在此可使用任何數目的通訊頻道。

根據本發明之其它技術態樣，輔助通訊連結 314 可為來自於安全服務 306 及網路安全模組 304 的單向通訊，或是安全服務與網路安全模組之間的雙向通訊連結。此外，透過輔助通訊連結 314，可從安全服務 306 下載如上所述之軟體更新或修補程式。

雖然網路安全模組 304 係介於電腦 302 與網際網路 110 之間，但網路安全模組的實際設置方式可以有所變化。無論是何種方式，網路安全模組 304 均會被電腦 302 視為信任的單元。根據一實施例，網路安全模組 304 係位在電腦 302 之外並連上網路 110 和電腦 302 的硬體裝置(有時稱作"dongle")。在另一種實施方式裡，網路安全模組 304

可以和電腦 302 整合在一起而成為一個硬體單元，或是做為電腦網路介面內的子單元。當電腦 302 經由無線連線連上網路 110 時，將網路安全模組 304 整合在電腦 302 內，或是當作電腦網路介面的子單元，均特別有用。

根據本發明之另一實施例，網路安全模組可以當作電腦 302 之某一單元內的邏輯電路—例如微程式碼(microcoding)或韌體，其中包括但不限於：處理器、圖形處理單元、北橋或南橋。在另一實施例中，網路安全模組可為軟體模組，其與作業系統協同運作或成為作業系統的一部分，或是做為安裝在電腦 302 上的獨立應用程式。以軟體形式來實作的網路安全模組 304 可在電腦 302 內的第二個處理器上進行操作。因此，網路安全模組 304 不應被限制在特定實施例。

在此需特別說明的是：本發明所獲致的諸項優點係在於系統會縮減許多電腦攻擊程式的影響。舉例而言，熟習相關技藝者當能瞭解，拒絕服務(denial of service, DOS)型攻擊係試圖以網路要求來摧垮電腦，直到電腦耗盡其資源並當機為止；或是，使電腦錯誤地進入模糊狀態而更容易受到外部攻擊/攻擊程式的不良影響。然而，利用網路安全模組 304 藉由執行保護安全措施來回應安全服務 306，上述包括潛在摧垮式網路要求在內的攻擊程式將無法接近電腦 302。

為了更加瞭解上述單元如何運作而能為電腦 302 提供更強化的安全性，以下將參照對應於事件的時間線所繪

示的情境範例來加以說明。第 4A 圖與第 4B 圖係方塊圖，其繪示用來說明本發明之各項單元運作的示範性時間線。確切而言，第 4A 圖繪示時間線 400 範例的方塊圖，其說明本發明如何能縮小電腦 302 相對於在網路 110 上所散佈的新電腦攻擊程式的安全性漏洞 406。在此需注意的是：以下的說明僅以攻擊作業系統的電腦攻擊程式為例，其不應被解讀為本發明之限制。本發明實則可應用於保護電腦系統上的程式碼模組、服務，甚至可保護硬體裝置。

如時間線 400 所示，在事件 402 處，惡意人士將一種新的電腦攻擊程式散佈在網路 110 上。此散佈行動會開啟屬於新的電腦攻擊程式之攻擊目標並已連上網路 110 的電腦之安全性漏洞空窗期 406。在事件 404 處，新的電腦攻擊程式以上述方式被作業系統提供者或防毒軟體提供者偵測到。

在事件 408 處，在偵測到存在新的電腦攻擊程式之後，即使尚未確定該攻擊程式的特性或攻擊模式，作業系統提供者會經由安全服務 306 發佈安全性資訊。在典型情況下，當發現到電腦攻擊程式且尚不知其特性、影響範圍或攻擊模式時，安全服務會將所有似乎會被影響的電腦系統之安全性層級設定在紅色層級—亦即完全封鎖。在方塊 410 處，網路安全模組 304 會透過定期要求或安全佈告而取得安全性資訊，並執行對應的安全措施—在此例中為完全封鎖。在執行來自於安全服務 306 的安全措施之後，屬於攻擊目標的電腦之安全性漏洞空窗期 406 會被有效地關

閉。

相較於第 2B 圖所示之安全性漏洞空窗期 230，安全性漏洞空窗期 406 較短，因而可以縮短屬於新的電腦攻擊程式之攻擊目標的電腦系統的暴露時間。顯然地，安全性漏洞(例如安全性漏洞空窗期 406)的實際開啟時間長度係取決於少數幾個因素。在偵測到電腦攻擊程式之前所歷經的時間長度是其中一個因素。如上所述，新的電腦攻擊程式一般是在散佈後的十五分鐘到數小時之內會被偵測到。第二個因素係網路安全模組 304 從安全服務 306 取得安全性資訊所需花費的時間長度；此因素的變化程度大於第一個因素的變化程度。若網路安全模組 304 可以持續取得安全性資訊，則只需數秒鐘即可取得安全性資訊，並執行對應的安全措施。然而，若網路安全模組 304 無法持續與安全服務 306 進行聯繫，或定期取得安全性資訊的時間規劃過長，則執行保護安全措施會需要很長的時間。根據本發明之技術態樣，若有一段時間網路安全模組 304 沒有和安全服務 306 取得聯繫，則網路安全模組會回到預設的完全封鎖狀態，並等待未來與安全服務進行聯繫。

在發佈初始安全性資訊之後，作業系統提供者或防毒軟體提供者通常會持續分析電腦攻擊程式，以便更加瞭解其運作方式及/或其所攻擊的電腦系統之特點。由此分析可以找到第二組或許較不嚴格的保護措施；存在安全性漏洞的電腦系統必須採取此保護措施，以避免感染到電腦攻擊程式。因此，在事件 412 處，已更新的安全性資訊會以

黃色安全性層級進行發佈，並確定用來封鎖處於危險的網路活動的保護措施—亦即部分封鎖。舉例而言，如上所述，保護安全措施可以是單純地封鎖特定範圍的通訊埠—其中包括來源及/或目的地埠口，或是停用安裝在受保護電腦系統上的電子郵件通訊埠、網頁瀏覽或其它導向作業系統、應用程式裝置驅動程式或類似程式的網路活動，同時容許其它網路活動自由地流通。在此需瞭解的是:「處於危險的」網路活動包括電腦系統受到攻擊程式威脅的網路活動，且不論電腦攻擊程式是攻擊電腦系統的安全漏洞，或是濫用適格的電腦系統特點。此外，「處於危險的」網路活動尚包括單方面由另一裝置針對電腦系統所發動的網路活動。換言之，「處於危險的」網路活動包括攻擊程式針對只是單純連上網路的電腦系統所發動的網路活動。

在事件414處，網路安全模組304取得已更新的安全性資訊，並執行對應的保護安全措施。在事件416處，當作業系統提供者及/或防毒軟體提供者建立可用的軟體更新程式之後，即會發佈另一項已更新的安全性資訊。若一個軟體更新程式—例如來自於作業系統提供者、防毒軟體提供者或應用程式提供者的更新程式—已安裝在電腦302上，則此項已更新的安全性資訊或許會將安全性層級認定為綠色層級。隨後，在事件418處取得上述另一項已更新的安全性資訊、此軟體更新安裝在電腦302上，同時網路安全模組304啟用自由的(即無限制的)網路存取。

第4B圖繪示另一種示範性時間線420的方塊圖，其

說明本發明如何能消除相對於在網路 110 上所散佈的電腦攻擊程式的安全性漏洞空窗期；尤其是一種利用先前找到的安全性漏洞而非全新攻擊的電腦攻擊程式。如上所述，利用先前已知安全性漏洞的攻擊比全新的攻擊更為常見。在事件 422 處，作業系統提供者在目前發行的作業系統內找到安全性漏洞。在事件 424 處，作業系統提供者發佈能減輕威脅的安全性資訊、設定安全性層級，並確認對應的保護安全措施，以對付找到的安全性漏洞所帶來的威脅。在第 4B 圖所示範例中，若安全性漏洞為連上網路 110 的電腦帶來極大的危險，則作業系統提供者會發佈安全性資訊，並將安全性層級設定在紅色層級，同時採取完全封鎖的安全措施。在事件 426 處，網路安全模組 304 取得最新的安全性資訊並執行完全封鎖措施。在此需注意的是：在修補程式或「修復」可供使用之前，即已先執行保護電腦 302 之安全性漏洞的安全措施。由於大部分的電腦攻擊程式均或多或少從分析修補程式所修正的安全性漏洞取得的資訊衍生而來，惡意人士會預先拒絕建立用來攻擊安全性漏洞之攻擊程式的機會，因而不會開啟安全性漏洞空窗期。此結果顯然對電腦使用者非常有利，尤其是當網路安全模組沒有執行安全措施時；請參照第 2A 圖所示對應的時間線 200。

針對電腦攻擊程式進行進一步的分析後，作業系統經常可以確定一組較不嚴格的保護措施，使連上網路的電腦不會受到電腦攻擊程式的攻擊。因此，如第 4B 圖所示，

在事件428處會發佈已更新的安全性佈告、將安全性層級設定為黃色層級，且包含特別針對受到威脅的安全性漏洞的對應保護安全措施—亦即部分封鎖，同時啟動其它所有網路活動。如此，在事件430處會取得已更新的安全性資訊，且網路安全模組304會執行部分封鎖。

一旦作業系統修補程式或防毒軟體更新程式可供使用，若將此類程式安裝在電腦302上，其可保護電腦302，使電腦的安全性漏洞不會成為電腦攻擊程式的攻擊目標；在事件432處，作業系統提供者發佈資訊並指出：一旦安裝完畢，網路安全模組即容許自由的網路存取動作，亦即在安裝修補程式之後，網路安全模組會將安全性層級設定為綠色層級。同樣地，在事件434處，當修補程式或防毒更新程式在電腦302上完成安裝之後，網路安全模組304會啟用自由存取。

第5圖為流程圖，其繪示根據發佈的安全性資訊來動態控制電腦之網路存取的副程式範例500。第5圖包含兩個啟始端點，其中啟始端點502相當於網路安全模組304的起點，啟始端點520則相當於從電腦系統302接收更新通知。首先從啟始端點502開始並進行到方塊504，網路安全模組304會執行完全封鎖的相關安全措施。如上所述，當處於完全封鎖時，電腦會被限制只能與包括安全服務306在內的已知信任的網路位置進行通訊，以便取得最新的安全性狀態資訊及任何可用的更新資訊。

在方塊506處，網路安全模組304從安全服務306

取得對應於電腦目前組態的安全性資訊。根據本發明之技術態樣，網路安全模組 304 可藉由向安全服務發出取得安全性資訊之要求而從安全服務取得最新的安全性資訊。在另一種實施方式當中，網路安全模組 304 可經由輔助通訊連結或網路上的播送，而從安全服務 306 的播送取得最新的安全性資訊。

在決定方塊 508 處，網路安全模組 304 會根據從安全服務 306 取得之最新的安全性資訊來判斷目前所執行的安全措施及對應的安全性層級是否與取得的安全性資訊一樣新。根據本發明之一技術態樣，此判斷係針對網路安全模組目前所儲存的電腦系統修訂資訊與安全服務所發佈的最新修訂資訊之間進行簡單的比對而做成。

在方塊 510 處，若目前所執行的安全措施不是最新的，則網路安全模組會根據其已儲存電腦系統之相關資訊來取得該電腦系統之安全措施。在另一種實施方式中(圖中未繪示)，安全措施可包含於取得的安全性資訊當中。在方塊 512 處，一旦網路安全模組 304 取得安全措施，其會執行該安全措施並設定對應的安全性層級，亦即紅色、黃色或綠色等安全性層級。

在方塊 514 處，執行電腦系統的安全措施之後，或是若目前為電腦系統所執行的安全措施是最新的，則網路安全模組 304 會進入延遲狀態。此延遲狀態係對應於網路安全模組 304 定期向安全服務 306 查詢以取得最新的安全性資訊的時間週期。在延遲一段預設的時間之後，處理程

序會回到方塊 506；在此，從安全服務 306 取得最新安全性資訊的程序會重複被執行，以確定目前為電腦系統所執行的安全措施是否是最新的，同時執行任何新的安全措施。

如第 5 圖所示，由於示範性副程式 500 的設計方式係使其能持續運作來保護電腦 302 免於受到電腦程式攻擊，因此副程式 500 沒有結束端點。然而，熟習相關技藝者當能瞭解，若網路安全模組 304 的電源被關閉而未連上示範性網路環境 300，或如上述方式由使用者自行停用，則副程式 500 將會終止。

參照另一啟始端點 520，此進入點係代表網路安全模組 304 從電腦系統接收到更新通知時的情況。如上所述，適於利用本發明的應用程式會通知網路安全模組 304 關於目前的修訂資訊，並做為針對電腦系統進行更新的其中一個步驟。舉例而言，在進行防毒軟體更新時，其中一個步驟是向網路安全模組 304 發出通知，以告知網路安全模組 304 關於目前的修訂資訊。因此，在方塊 522 處，網路安全模組 304 會接收到更新通知。

在方塊 524 處，網路安全模組 304 會儲存更新通知資訊，以供稍後在判斷目前所執行的安全措施是否是最新時使用。作業系統更新和其它程式碼模組更新均適於提供通知給網路安全模組 304，使安全系統得以在持有充分資訊下做出關於保護任一電腦系統所需要的適當安全措施之判斷。

完成儲存資訊之後，副程式 500 會進行到方塊 506；

在此會開始進行從安全服務306取得最新的安全性資訊的步驟，並以上述方式確定目前為電腦系統所執行的安全措施是否是最新的，同時執行任何新的安全措施。在另一種實施方式中(圖中未繪示)，在方塊524處接收到已更新的電腦系統資訊之後，網路安全模組會在目前的延遲狀態結束之前等待取得安全性狀態資訊。

第6圖為示範性副程式600的流程圖，該副程式係用於播送網路安全模組—例如示範性網路環境300內的網路安全模組304—所需要的安全性資訊。從方塊602開始，安全服務306從各種來源取得安全性相關資訊。舉例而言，安全服務306通常會從作業系統提供者和防毒軟體提供者取得關於最新修訂、修補程式和可用的更新等資訊，以及各種不同的修補程式和更新所要解決的電腦攻擊程式及/或安全性漏洞。安全性相關資訊亦可經由輪詢(poll)其它來源來取得，其中包括各種政府機構、安全性專家或類似來源。

在方塊604處，安全服務306取得連上網路110的電腦系統之安全性漏洞的相關資訊。此資訊可能來自於作業系統提供者、防毒軟體提供者，或其它偵測到安全性漏洞的人士。在方塊606處，安全服務306會根據安全性漏洞所引發的威脅來判斷安全性層級—例如紅色、黃色和綠色層級，以及由網路安全模組—例如網路安全模組304—執行的保護措施，以使受到影響的電腦能免於遭到電腦攻擊程式攻擊其安全性漏洞。

在方塊606處，安全服務306會以上述方式將包含安全性層級與對應保護安全措施在內的安全性佈告播送到連上網路110的網路安全模組。如上所述，安全服務306可以透過發出全網域播送到所有的網路安全模組，以進行安全性佈告之播送。吾人可選擇利用上述保證傳輸來經由網路110進行全網域播送，或是透過網路環境300當中連上輔助通訊連結314的網路安全裝置來進行全網域播送。送出安全性佈告之後，副程式600隨即終止。

第7圖係繪示安全服務306所實作的副程式範例700之流程圖，該副程式能接收並回應來自於網路安全模組304的安全性資訊之要求。從方塊702處開始，安全服務會接收來自於網路安全裝置304的安全性資訊要求。如上所述，安全性資訊要求可以包含對應於電腦目前組態的資訊。

在方塊704處，根據網路安全模組所提供的安全性資訊要求當中的特定電腦組態資訊，安全服務306會找出對應於該安全性資訊要求當中的電腦目前組態資訊之相關安全性資訊。

根據一實施例，安全服務306係藉由確定根據電腦組態資訊來保護電腦302時所需要的保護安全措施來找出相關的安全性資訊。根據另一實施例，安全服務306係藉由傳回所有對應於特定電腦組態而供網路安全模組進行進一步處理的安全性資訊來判斷應執行何種保護安全措施。在另一實施例中，安全服務306係藉著傳回對應於特定電

腦組態的所有安全性資訊，而後再從網路安全裝置轉送到電腦 302，以使電腦能告知網路安全模組應執行何種保護安全措施。吾人亦可使用上述實施方式的其它組合或其它系統。因此，本發明不應被解讀限制在任何一種特定的實施例。

在方塊 706 處，安全服務 306 會將相關的安全性資訊傳回給提出要求的網路安全模組 304。隨後，副程式 700 終止。

第 8 圖係繪示網路安全模組 304 所實作的方法 800 流程圖，該方法能根據取自安全服務 306 的安全措施來控制電腦 302 與網路之間的網路流通。從方塊 802 開始，網路安全模組 304 接收網路流通，其中包括送往電腦 302 的網路流通，以及從電腦送出的網路流通。

在抉擇方塊 804 處係確定網路流通是否是從信任的網路位置送出，或送往信任的網路位置—例如安全服務、防毒軟體提供者、作業系統提供者或類似來源。若網路流通是來自或送往信任的位置，則副程式會進行到方塊 810；在此容許網路交流通過網路安全模組 304，而後副程式 800 終止。然而，若網路流通不是來自或送往信任的網路位置，則副程式進行到抉擇方塊 806。

在抉擇方塊 806 處會做出關於網路流通是否受到目前所執行的安全措施之限制的抉擇。若網路流通未受到目前執行的安全措施的限制，則副程式進行到方塊 810；在此容許網路流通經過網路安全模組 304，隨後副程式 800

終止。然而，若網路流通已根據目前執行的安全措施而受到限制，則副程式進行到方塊 808；在此不容許網路流通經過網路安全模組 304。隨後，副程式 800 終止。

雖然網路安全模組 304 係位在電腦 302 與網際網路 110 之間，但網路安全模組的實施例可以有所變化。根據一實施例，網路安全模組 304 可為電腦 302 外部的硬體裝置，並連接到網際網路 110 與電腦 302。第 9 圖係繪示以電腦 302 外部硬體裝置實作的網路安全模組 304 範例之示意圖。

如第 9 圖所示，做為外部裝置的網路安全模組 304 具有連接到網路 110 的連線 902，以及連接到電腦 302 的對應連線 904。電腦 302 與網路 110 之間的所有網路活動均是在連接到電腦的連線 904 上進行。圖中所示網路安全模組 304 亦具備輔助電腦連線 918，其負責在電腦 302 與網路安全模組之間傳遞資訊。圖中所示網路安全裝置 304 另包含啟用/停用開關 906、狀態指示器 910-916，以及連接到外部電源的備用連線 908。

如上所述，有時會需要使網路安全模組停止執行其目前的安全措施。根據第 9 圖所示實施例，啟用/停用開關 906 係一種雙態開關：當需要忽略目前的安全措施時，啟用/停用開關 906 可以停用網路安全模組 304；啟用/停用開關 906 亦可啟用網路安全模組 304，使其能執行其已從安全服務 306 取得的當前安全措施。

狀態指示器 910-916 包含網路安全模組目前狀態的

視覺化指示。如上所述，狀態指示器僅以提供訊息為目的，其為電腦使用者提供關於網路安全模組 304 所執行的保護安全措施的提示。每一個指示器均對應於一個特定的安全性狀態。舉例而言，狀態指示器 910 可對應於紅色安全性層級，其意義為完全封鎖網路活動，並且在網路安全模組 304 正在執行完全封鎖時，狀態指示器會發出紅光。狀態指示器 912 可對應於黃色安全性層級，其意義為部分封鎖網路活動，並且在網路安全模組 304 正在執行部分封鎖時，狀態指示器會發出黃光。同樣地，狀態指示器 914 可對應於綠色安全性層級，即自由使用網路，並且在網路安全模組 304 容許使用未受限制的網路時，狀態指示器會發出綠光。狀態指示器 916 可對應於網路安全模組 304 的啟用/停用狀態，而當網路安全模組 304 被停用時會發出如紅色的閃光。

雖然本發明之實施例可如第 9 圖所示，但其僅為舉例說明；第 9 圖所示實施例有各種不脫離本發明之範圍的修飾及替換方式。因此，本發明不應被解讀為限定在任何一個實施例。

在另一實施例(圖中未繪示)中，網路安全模組 304 可為整合在電腦 302 內的元件，或是電腦網路介面內的子元件。當電腦 302 經由無線連線連上網際網路 110 時，這兩種實施方式特別有用。在另一種實施例中，網路安全模組 304 可為整合在作業系統內的軟體模組，或是安裝在電腦 302 上的單獨模組。因此，網路安全模組 304 不應被解

讀為只限定在特定的實體或邏輯實施方式。

第10圖為根據本發明建構的網路安全模組304之邏輯單元的方塊圖。網路安全模組304內包含記憶體1002、安全狀態指示器模組1004、比對模組1006、安全執行模組1008、更新要求模組1010、網路連線1012、電腦連線1014、備用電腦連線1018，以及編碼器/解碼器模組1020。

記憶體1002—包括揮發性與非揮發性記憶區—係用來儲存網路安全模組304所執行的目前安全措施。記憶體1002亦可儲存提供給網路安全模組304的組態資訊，其中包括作業系統、防毒軟體及簽章、應用程式等目前的修訂資訊及類似資訊。其它資訊亦可存放在記憶體1002內，其中包括信任位置的位址、更新來源及類似資訊。如信任位置之位址之類的資訊比較可能存放在非揮發性記憶體內。

安全狀態指示器模組1004係為電腦使用者指出網路安全模組304目前的安全性狀態。舉例而言，當網路安全模組304係如第9圖所示之實體裝置型態時，安全狀態指示器模組1004會根據網路安全模組當前的安全狀態來控制狀態指示器910-916。

比對模組1006會針對記憶體1002所儲存的安全性資訊與從安全服務306取得的安全性資訊進行比對，藉以判斷存放在記憶體1002內的安全性資訊是否對電腦目前組態而言為最新的。安全執行模組1008係藉由執行安全措施來保護電腦302免於受到已知威脅的元件。因此，安全執行模組1008會根據存放在記憶體1002內的安全措施來

控制電腦 302 與網路 110 之間的網路活動流通。

更新要求模組 1010 係用於輪詢系統，其會定期向安全服務 306 要求最新的安全性資訊。在推式系統(push system)當中，更新要求模組 1010 可當作從安全服務接收安全性資訊的接收器，並和比對模組 1006 協同運作，以找到根據從安全服務 306 接收到的資訊來充分保護電腦 302 的保護安全措施。在另一種實施方式中，更新要求模組可以和電腦 302 聯繫，以確立/找到根據從安全服務 306 接收到的資訊來充分保護電腦 302 的保護安全措施。網路安全模組 304 的所有元件均是經由共用的系統匯流排 1016 相互連接。

編碼器/解碼器模組 1020 係用於針對網路安全模組 304 與安全服務 306 之間的安全通訊以及電腦 302 與網路安全模組之間的安全通訊進行編碼和解碼。經過編碼器/解碼器模組 1020 解碼的資訊會提供給安全執行模組 1008，以執行目前的安全性資訊。

根據一實施例，電腦 302 與網路安全模組 304 之間的安全通訊會經由輔助電腦連線 1018 進行傳送。然而，本發明不應被解讀為必須包含輔助電腦連線 1018。在另一種實施例中，網路安全模組 304 僅利用主要電腦連線 1014 來聯繫電腦 302。

雖然以上已描述網路安全模組 304 的個別元件，但應瞭解的是，上述元件僅為邏輯元件，在實作過程中，其可結合在一起或與其它未在此說明的元件結合。因此，上

述元件僅為舉例說明，而不應被解讀為本發明之限制條件。

雖然上述網路安全模組能以單獨運作或與防毒軟體共同運作的方式來保護電腦，使其免於受到許多電腦攻擊程式/攻擊的破壞，但在某些情況下，某些攻擊程式或許能夠繞過網路安全模組及/或防毒軟體。在特定情況中，惡意人士用來攻擊計算裝置的其中一種技術係利用受感染的電腦/攻擊程式起源與成為攻擊對象的計算裝置之間的安全通訊，使攻擊程式隔離而不會被偵測到。第 11 圖為方塊圖，其繪示如何利用安全通訊將電腦攻擊程式傳送到計算裝置。

參照第 11 圖，在說明如何利用安全通訊將電腦攻擊程式傳送到計算裝置的範例時，假設電腦 102 上的惡意人士備有一種攻擊程式。為了要感染另一台電腦—例如電腦 1104，該惡意人士可能會以適格的資源/內容傳送攻擊程式 112 給他人，但卻經由安全通訊進行傳送。如熟習相關技藝者所知，安全通訊通常會經過公開或私密的密碼金鑰之加密處理，使解密金鑰(私密金鑰)的擁有人才能解密並檢視安全通訊的內容。安全通訊協定的範例包括 SSL 協定與傳輸層安全(Transport Layer Security, TLS)協定。

繼續說明本例：未察覺的使用者會經由計算裝置 1104 被欺騙而相信攻擊程式 112 確實是適格的內容，並從電腦 102 要求該攻擊程式。電腦 102 和計算裝置 1104 會協商，並交換用來針對攻擊程式 112 進行加密和解密的密碼金鑰。隨後，如箭號 1108 所示，傳輸編碼器 1106 會針對

該攻擊程式進行編碼以供傳輸，並經由網路 110 而將經過加密的攻擊程式安全地傳送給計算裝置 1104。由於攻擊程式 122 是以加密狀態被傳送，因此其非常可能會通過網路安全模組 304(圖中未繪示)及任何的防毒軟體。到達計算裝置 1104 後，傳輸解碼器模組 1110 會針對安全通訊進行解碼/解密，並提供到瀏覽器顯示模組 1112。熟習相關技藝者當能瞭解，傳輸解碼器模組 1110 經常是瀏覽器顯示模組 1112 整體的一部分。顯示攻擊程式後，瀏覽器顯示模組 1112 會啟用該攻擊程式 112 來感染計算裝置 1104。

根據本發明之技術態樣，網路安全模組 304 可用來保護計算裝置，使其免於受到經由安全通訊傳遞的電腦攻擊程式之破壞。再次參照第 10 圖，網路安全模組 304 會經由輔助電腦連線 1018 而從計算裝置取得針對安全通訊進行解密所需要的密碼金鑰。一旦取得密碼金鑰，編碼器/解碼器模組 1020 會暫時針對安全通訊進行解碼以供處理。若安全通訊被發現違反網路安全模組 304 所執行的安全措施，或發現該安全通訊是一個攻擊程式，則不容許該安全通訊到達計算裝置 1104。然而，若安全通訊沒有違反所執行的安全措施，而且不是一個攻擊程式，則會容許該安全通訊被送往計算裝置 1104。關於上述技術特點，以下將會進一步詳細解說。

根據本發明之技術態樣，輔助電腦連線 1018(第 10 圖)可以是通往計算裝置 1104 的各種通訊管道其中之一。舉例而言，輔助電腦連線 1018 可為通用序列埠(Universal

Serial Bus, USB)連線、IEEE 1394連線，或標準化的串列或平行資料連線。如上所述，輔助電腦連線1018的其中一項目的係提供一種通訊管道，讓網路安全模組304能經由該通訊管道而從傳輸解碼器1110取得解密金鑰，以便暫時將安全通訊解密。因此，在另一種實施方式中，輔助電腦連線1018亦可為計算裝置與網路110之間進行網路活動所經過的電腦連線1014。根據此實施例，電腦連線1014與輔助電腦連線1018之間的差異係在於邏輯上差異，而非實體上的差異。

第12圖為示範性環境1200之方塊圖，其根據本發明之技術態樣繪示網路安全模組304如何能使計算裝置1104免於受到經由安全通訊傳送到該計算裝置的電腦攻擊程式112之攻擊。如箭號1108所示，如同第11圖所示實施例，電腦102上的惡意人士試圖經由安全通訊而將電腦攻擊程式傳遞到計算裝置。然而，位在網路110與計算裝置1104之間的的網路安全模組304會先取得安全通訊。網路安全模組304會查驗內送的網路活動，藉以判斷是否有任何通訊是安全通訊，並做為執行關於目前安全性層級的安全措施的一部分，或單純是進行當中的安全性預警。

如箭號1202所示，偵測到安全通訊之後，網路安全模組304會透過輔助電腦連線1018，向計算裝置1102上的傳輸解碼器模組1110提出取得解密金鑰的要求。網路安全模組304係利用此解密金鑰來暫時將安全通訊解密，並根據網路安全模組所執行的任何一種安全措施來處理經過

解密的通訊資料。根據本發明之其它技術態樣，網路安全模組 304 亦可配合防毒軟體之運作，將暫時解密的通訊資料傳送到防毒軟體，以供其評估攻擊程式/病毒。

如箭號 1204 所示，當偵測到安全通訊是執行的安全措施所禁止的網路活動後，或防毒軟體偵測到該安全通訊為攻擊程式後，網路安全模組 304 會禁止該安全通訊/攻擊程式到達計算裝置 1104。以此方式，即使是透過安全通訊管道來傳送通訊，計算裝置 1104 亦可得到保護。在另一種方式中，若安全通訊沒有違反任何一種執行的安全措施，而且不是攻擊程式，則該安全通訊會被轉送到計算裝置 1104。

在以上針對第 11 圖和第 12 圖所作的說明內容當中，雖然傳輸解碼器 1110 係與瀏覽器顯示模組 1112 分離的單獨模組，但其僅為舉例說明。熟習相關技藝者當能瞭解，傳輸解碼器 1110 經常是計算裝置上的瀏覽器顯示模組 1112 的整合元件。

第 13A 圖及第 13B 圖繪示副程式範例 1300 之方塊圖，該副程式係根據本發明之技術態樣來偵測及處理安全通訊。在此需注意的是，雖然可在網路安全模組 304 上執行示範性副程式 1300，其亦可單獨執行，並以配合瀏覽器顯示模組 1112 共同運作的軟體模組來執行，以保護計算裝置 1104 免於受到攻擊程式 112 的破壞。

從方塊 1302 開始(第 13A 圖)，示範性副程式 1300 監視網路活動—特別是內送的網路活動。偵測到內送網路

活動時，在抉擇方塊1304處會判斷該網路活動是否是送往受保護計算裝置的安全通訊。若該網路活動不是一個送往受保護計算裝置的安全通訊，則在方塊1306處，該網路活動會被轉送到受保護的計算裝置。接著，處理流程回到方塊1302，以進行其它的網路活動監視。儘管圖中未繪示，但其它處理過程仍可能出現在不安全的網路活動。舉例而言，若在網路安全模組—例如網路安全模組 304—上執行示範性副程式1300，則可能會有其它處理過程，例如判斷網路活動是否違反網路安全模組所執行的任何一種安全措施。以上已說明此種關於處理不安全網路活動的方式。

若網路活動是安全通訊，則在方塊1308處會取得將該安全通訊解密所需要用到的解密金鑰。在方塊1310處會利用取得的解密金鑰來針對該安全通訊進行暫時解密。接著，在抉擇方塊1312(第13B圖)處會判斷經過解密的通訊是否受到網路安全模組304所執行的安全措施的禁止。若該通訊代表受到禁止的網路活動，則在方塊1314處，該安全通訊會被禁止，亦即不會被轉送到計算裝置。接著，副程式1300回到方塊1302處(第13A圖)，並繼續監視網路活動。

若經過解密的通訊沒有受到所執行的安全措施禁止，則在抉擇方塊1316處會另外判斷已解密的通訊是否為攻擊程式。如上所述，網路安全模組304可以配合外部防毒軟體共同運作。在此環境中，網路安全模組304會將暫時解密的通訊傳送到防毒軟體，以供查驗其是否為攻擊程

式或已被攻擊程式感染。若已解密的通訊經判斷為攻擊程式，則在方塊 14314 處，該安全通訊會被禁止，且副程式 1300 回到方塊 14302(第 13A 圖)，並繼續監視網路活動。在另一種方式中，若已解密的通訊經判斷不是攻擊程式，則在方塊 1318 處，安全通訊會被轉送到計算裝置。接著，副程式 1300 回到方塊 1302(第 13A 圖)並繼續監視網路活動。

儘管以上已詳細解說並舉例說明包含本發明之較佳實施例在內的各式實施例，但應瞭解的是，在不脫離本發明之原則及範圍的前提下，存在各式不同的變更。

【圖式簡單說明】

第 1 圖為習知網路環境之示意圖，其中電腦攻擊程式通常散佈在所示網路上。

第 2A 圖和第 2B 圖為時間線之方塊圖，其分別繪示電腦系統相對於散佈在網路上之電腦攻擊程式的不同 VUL 空窗期。

第 3A 圖和第 3B 圖為網路化環境之示意圖，所示環境適於實施本發明之各式技術態樣。

第 4A 圖和第 4B 圖為時間線之示意圖，其繪示本發明如何縮小與電腦攻擊程式有關的 VUL 空窗期。

第 5 圖為符合本發明的副程式範例之流程圖，該副程式係根據發佈的安全性資訊來控制電腦系統之網路存取。

第 6 圖係根據本發明繪示安全服務所實作之副程式範例的

流程圖，該副程式能將網路安全模組所需要的安全資訊發佈於示範性網路化環境中。

第 7 圖係繪示安全服務所實作的副程式範例之流程圖，該副程式能接收並回應來自於網路安全模組的安全性資訊之要求。

第 8 圖係繪示網路安全模組所實作的方法流程圖，該方法能根據取自安全服務的安全措施來控制電腦與網路之間的網路交流。

第 9 圖係繪示以電腦外部硬體裝置實作的網路安全模組範例之示意圖。

第 10 圖為根據本發明建構的網路安全模組之邏輯單元的方塊圖。

第 11 圖為方塊圖，其繪示如何利用安全通訊將電腦攻擊程式傳送到計算裝置。

第 12 圖為方塊圖，其繪示網路安全模組如何能使計算裝置免於受到利用安全通訊傳送到該計算裝置的電腦攻擊程式之攻擊。

第 13A 圖和第 13B 圖繪示副程式範例之方塊圖，該副程式係根據本發明之技術態樣來偵測及處理安全通訊。

【主要元件符號說明】

100	網路環境	102-108	電腦
110	通訊網路	112	電腦攻擊程式
200	時間線	220	時間線

300 網路環境	302 電腦
304 網路安全模組	306 安全服務
308 防毒軟體服務	310 網路環境
312 接收裝置	314 輔助通訊連結
400 時間線	420 時間線
902 連線	904 連線
908 備用連線	910-916 狀態指示器
1002 記憶體	1004 安全狀態指示器模組
1006 比對模組	1008 安全執行模組
1010 更新要求模組	1012 網路連線
1014 電腦連線	1016 系統匯流排
1018 備用電腦連線	1020 編碼器/解碼器模組
1104 計算裝置	1106 傳輸編碼器
1110 傳輸解碼器模組	1112 瀏覽器顯示模組
1200 環境	

伍、中文發明摘要：

在此揭示一種網路安全模組，用於保護連接到通訊網路的計算裝置，使其免於受到經由安全通訊傳遞的已知安全性威脅。此種網路安全模組係以邏輯或實體方式介於受保護的電腦與通訊網路之間。當偵測到安全通訊後，上述網路安全模組會從計算裝置取得解密金鑰，以針對該安全通訊進行解密。隨後，上述網路安全模組根據該經過解密的通訊是否違反該網路安全模組所執行的保護安全措施來處理已解密的通訊。

陸、英文發明摘要：

A network security module for protecting computing devices connected to a communication net work from identified security threats communicated in a secured communication is presented. The network security module is interposed, either logically or physically, between the protected computer and the communication network. Upon detecting a secured communication, the network security module obtains a decryption key from the computing device to decrypt the secured communication. The network security module then processes the decrypted communication according to whether the decrypted communication violates protective security measures implemented by the network security module.

拾、申請專利範圍：

1.一種網路安全模組，其係介於一計算裝置與一網路之間，使該計算裝置與該網路之間的所有網路活動均會通過該網路安全模組，藉以保護該計算裝置免於受到該網路上所偵測到的安全威脅，該網路安全模組至少包含：

一計算裝置連線，其係用於將該網路安全模組連接到該計算裝置；

一網路連線，其係用於將該網路安全模組連接到該網路；

一解碼器模組，其係利用一取得的解密金鑰，暫時將一安全通訊解密；以及

一安全執行模組，其係藉由執行取得的安全措施來控制該計算裝置與該網路之間的網路活動，以便保護該計算裝置免於受到該網路上所偵測到的安全威脅。

2.如申請專利範圍第 1 項所述之網路安全模組，其中上述之安全執行模組係藉由取得該暫時解密的安全通訊，並根據該取得的安全措施來評估該暫時解密的安全通訊，以控制該計算裝置與該網路之間的網路活動。

3.如申請專利範圍第 1 項所述之網路安全模組，其中上述之解碼器模組取得該解密金鑰，並將來自於該計算裝置上的解碼模組的安全通訊暫時解密。

4.如申請專利範圍第 3 項所述之網路安全模組，其中更包含一輔助通訊連線，其係用於將該網路安全模組連接到該計算裝置，且其中該解碼器模組透過該輔助通訊連線而取得該解密金鑰，並將來自於該計算裝置上的解碼模組的安全通訊暫時解密。

5.如申請專利範圍第 1 項所述之網路安全模組，其中上述之安全通訊係依據安全套接字層(Secure Sockets Layer, SSL)協定以加密之。

6.如申請專利範圍第 1 項所述之網路安全模組，其中上述之安全通訊係依據傳輸層安全(Transport Layer Security)協定以加密之。

7.一種保護一計算裝置免於受到網路上所偵測到之安全威脅的方法，該方法係由介於該計算裝置與該網路之間的網路安全模組所執行，使該計算裝置與該網路之間的所有網路活動均會通過該網路安全模組，該方法至少包含：

取得保護安全措施，用於保護該計算裝置，使其免於受到所偵測到之安全威脅；

偵測送往該計算裝置的安全通訊；

將該安全通訊暫時解密；以及

針對該暫時被解密的安全通訊進行該保護安全措施。

8.如申請專利範圍第 7 項所述之方法，其中更包含從該計算裝置取得用於將該安全通訊解密的解密金鑰。

9.如申請專利範圍第 8 項所述之方法，其中上述之解密金鑰係經由該網路安全模組與該計算裝置之間的一輔助通訊連接而從該計算裝置取得。

10.如申請專利範圍第 9 項所述之方法，其中上述之解密金鑰係從該計算裝置上的解碼模組取得。

11.如申請專利範圍第 9 項所述之方法，其中上述之安全通訊係根據安全套接字層協定以加密之。

12.如申請專利範圍第 9 項所述之方法，其中上述之安全通訊係根據傳輸層安全協定以加密之。

13.如申請專利範圍第 7 項所述之方法，其中更包含從該計算裝置取得關於該計算裝置的組態資訊，且其中取得保護安全措施，其用於保護該計算裝置，使其免於受到所偵測到之安全威脅的步驟包含取得保護安全措施，並根據關於該計算裝置的組態資訊來保護該計算裝置。

14.一種網路安全模組，其係介於網路裝置與網路之間，使該網路裝置與該網路之間的所有網路活動均會通過該網路安全模組，藉以保護該網路裝置免於受到該網路上所偵測到的安全威脅，該網路安全模組至少包含：

一網路裝置連線，其係用於將該網路安全模組連接到該網路裝置；

一網路連線，其係用於將該網路安全模組連接到該網路；

一解碼器裝置，其係利用取得的解密金鑰，暫時將一安全通訊解密；以及

一安全執行裝置，其係藉由執行取得的安全措施來控制該網路裝置與該網路之間的網路活動，以便保護該網路裝置免於受到該網路上所偵測到的安全威脅。

15.如申請專利範圍第 14 項所述之網路安全模組，其中上述之安全執行裝置係從該解碼器裝置取得該暫時解密的安全通訊，並根據該取得的安全措施來評估該暫時解密的安全通訊，以控制該網路裝置與該網路之間的網路活動。

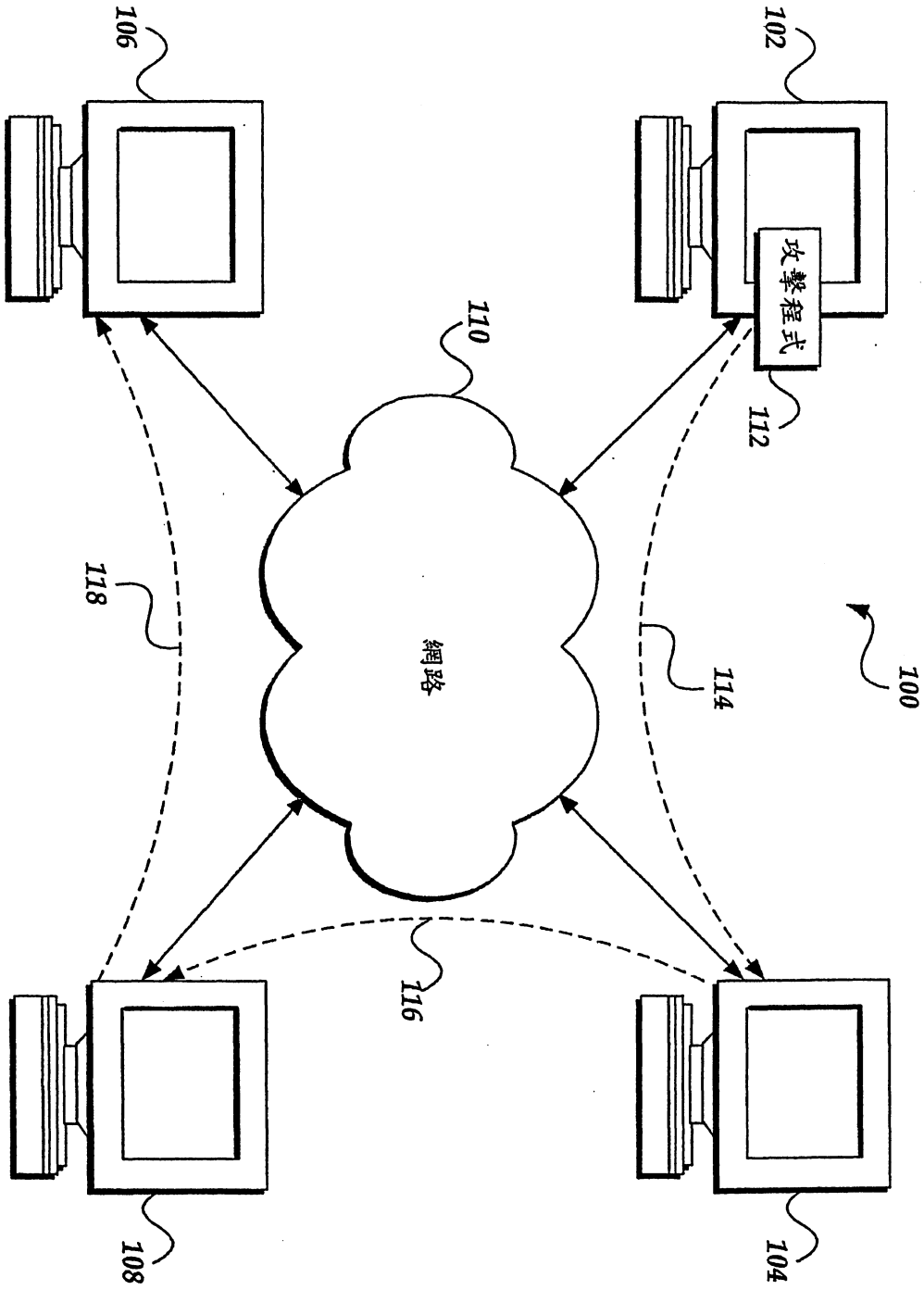
16.如申請專利範圍第 14 項所述之網路安全模組，其中上述之解碼器裝置取得該解密金鑰，並將來自於該網路裝置上的解碼模組的安全通訊暫時解密。

17.如申請專利範圍第 16 項所述之網路安全模組，其中更包含一輔助通訊連線，其係用於將該網路安全模組連接到該網路裝置，且其中該解碼器裝置透過該輔助通訊連線而取得該解密金鑰，並將來自於該網路裝置上的解碼模組的安全通訊暫時解密。

18.如申請專利範圍第 14 項所述之網路安全模組，其中上述之安全通訊係根據安全套接字層協定以加密之。

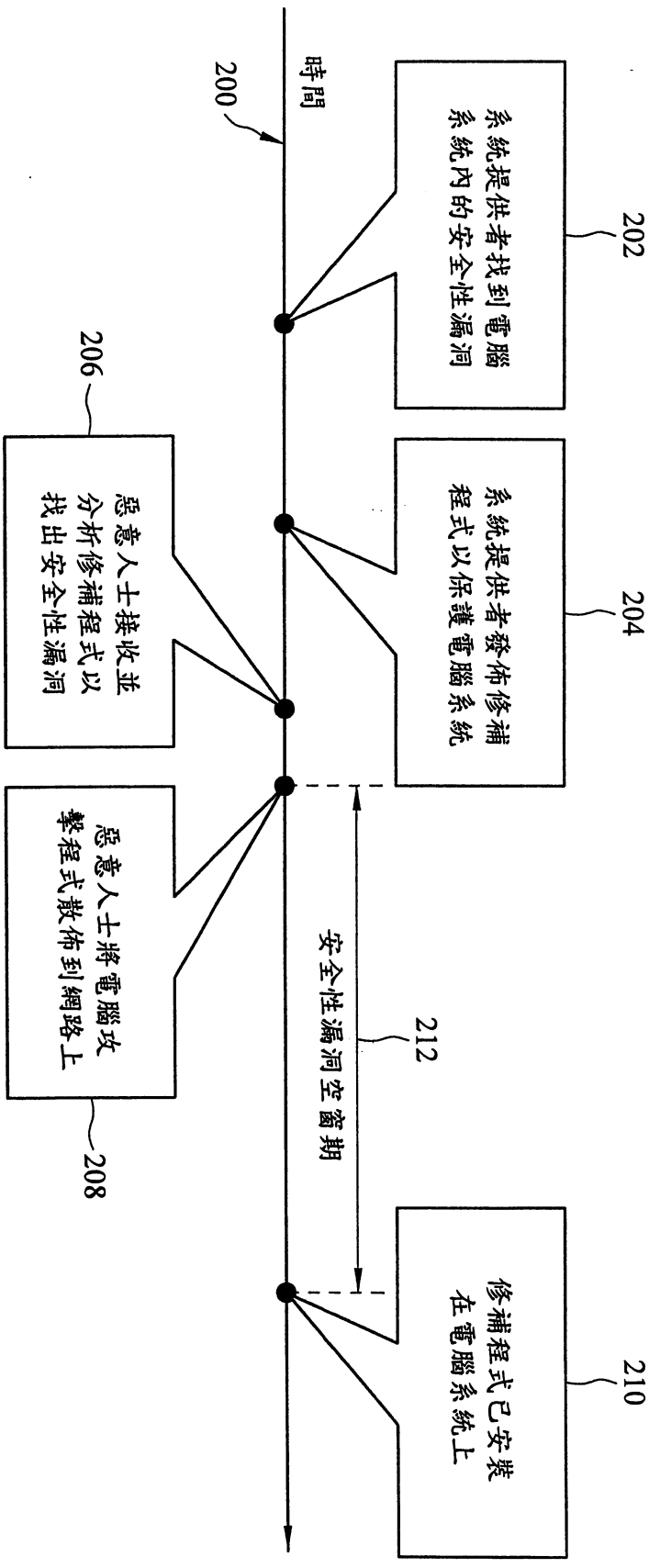
19.如申請專利範圍第 14 項所述之網路安全模組，其中上述之安全通訊係根據傳輸層安全協定以加密之。

200529002

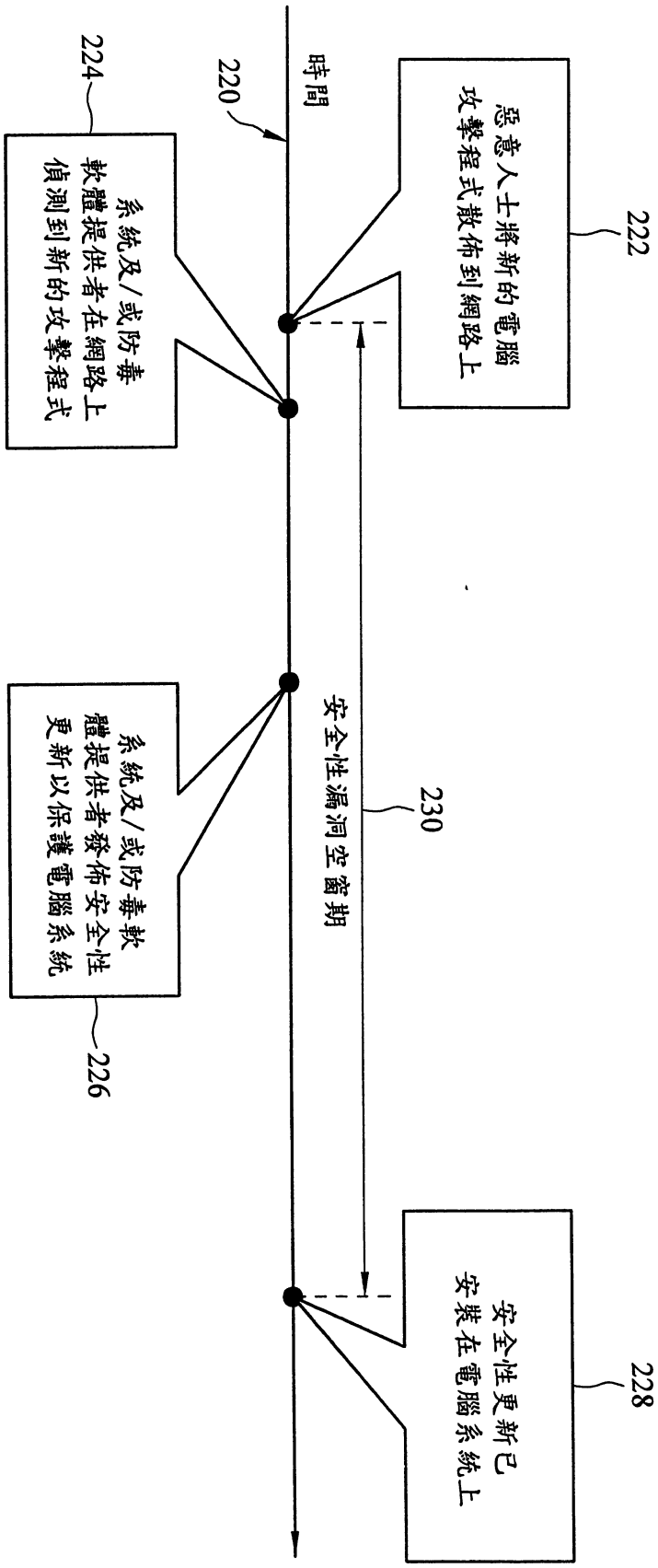


第 1 圖

200529002

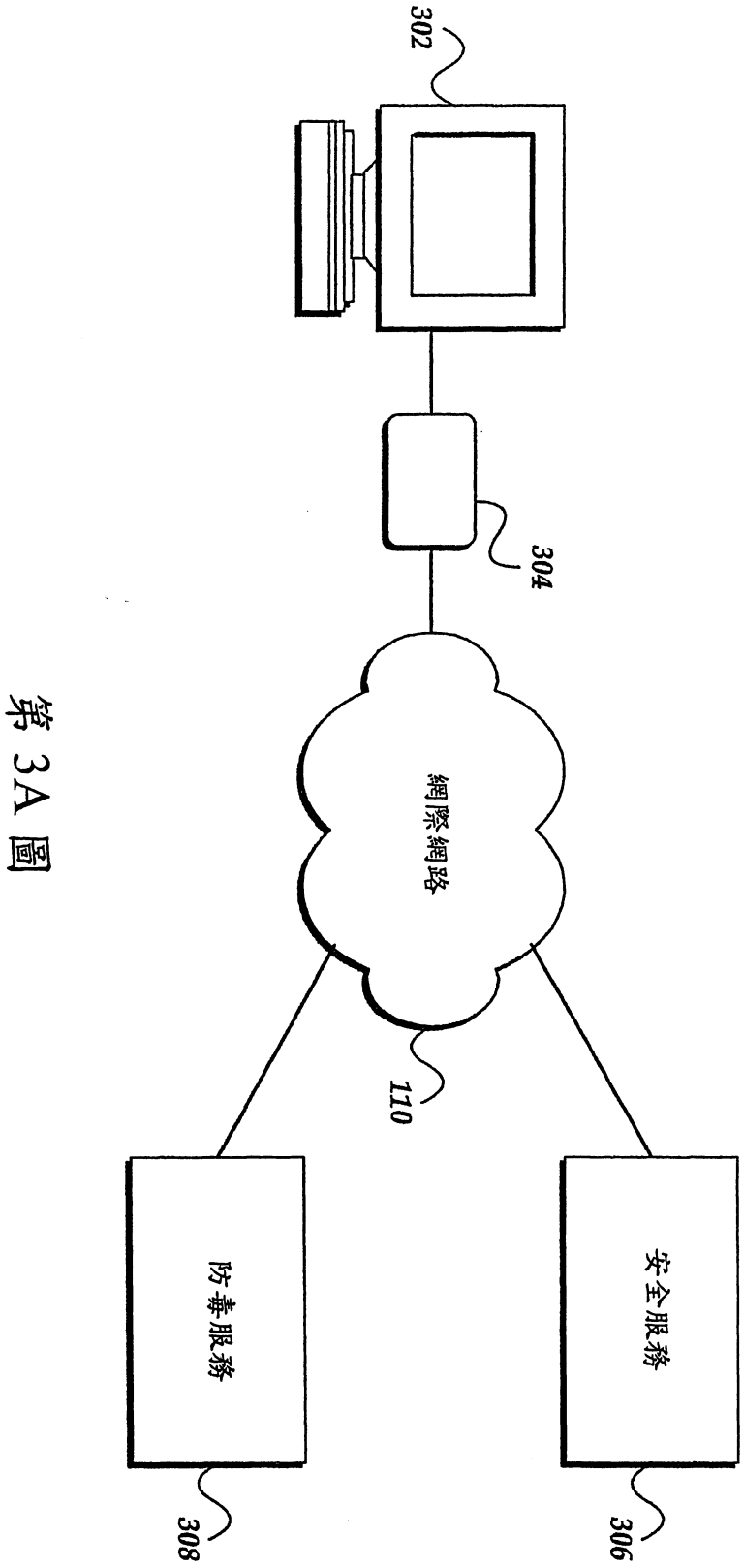


第 2A 圖


222
惡意人士將新的電腦攻擊程式散佈到網路上
時間
220
224
系統及/或防毒軟體提供者在網路上偵測到新的攻擊程式
安全性漏洞空窗期
230
系統及/或防毒軟體提供者發佈安全性更新以保護電腦系統
226
安全性更新已安裝在電腦系統上
228

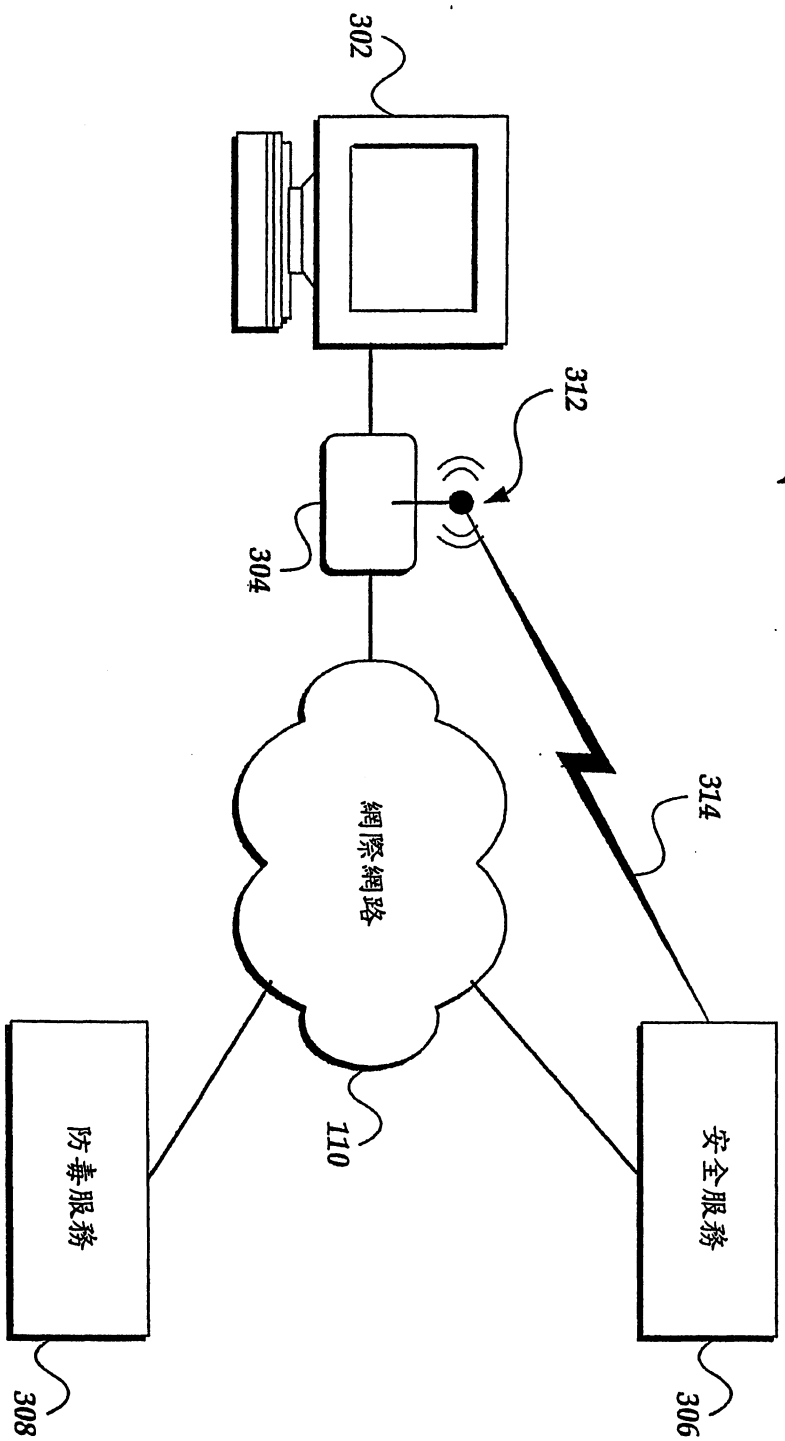
第 2B 圖

200529002



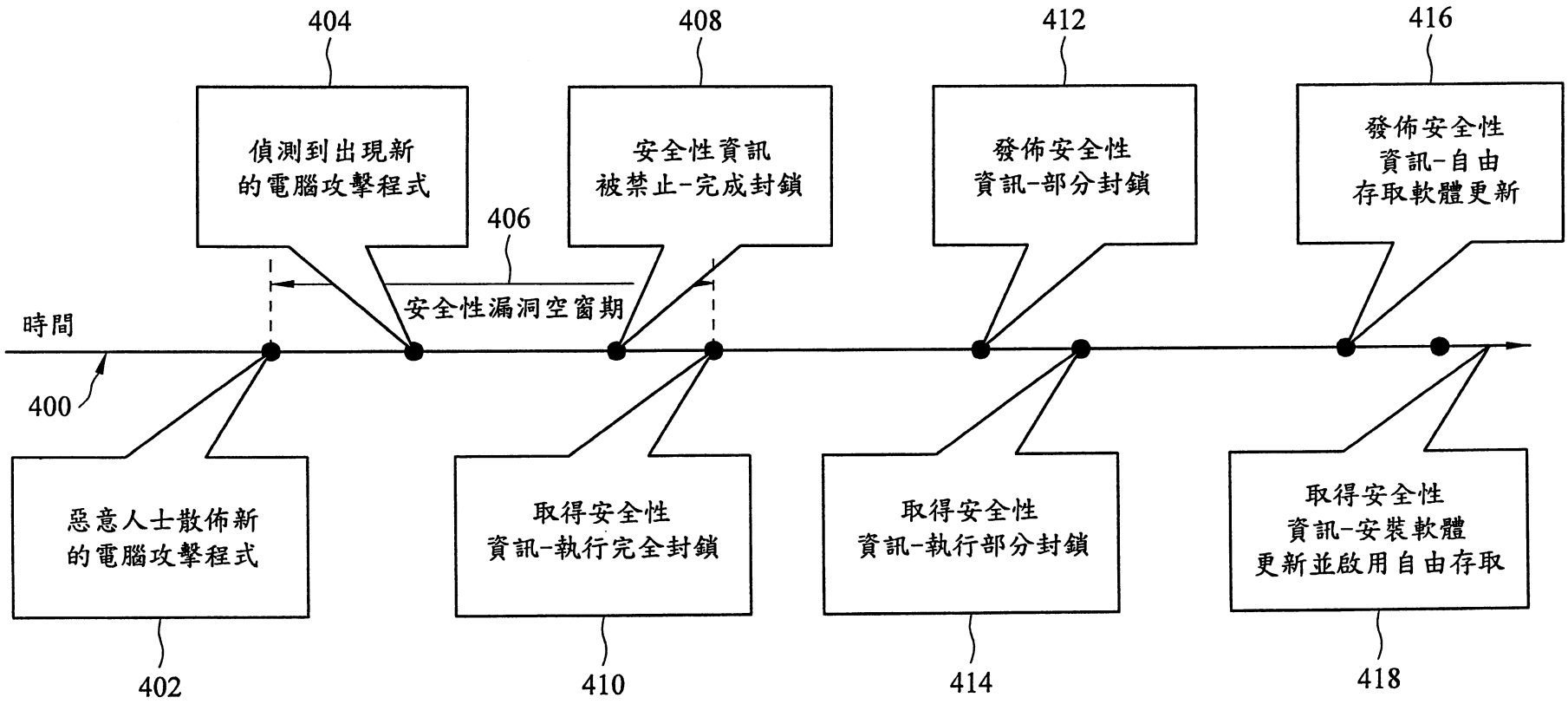
第 3A 圖

200529002



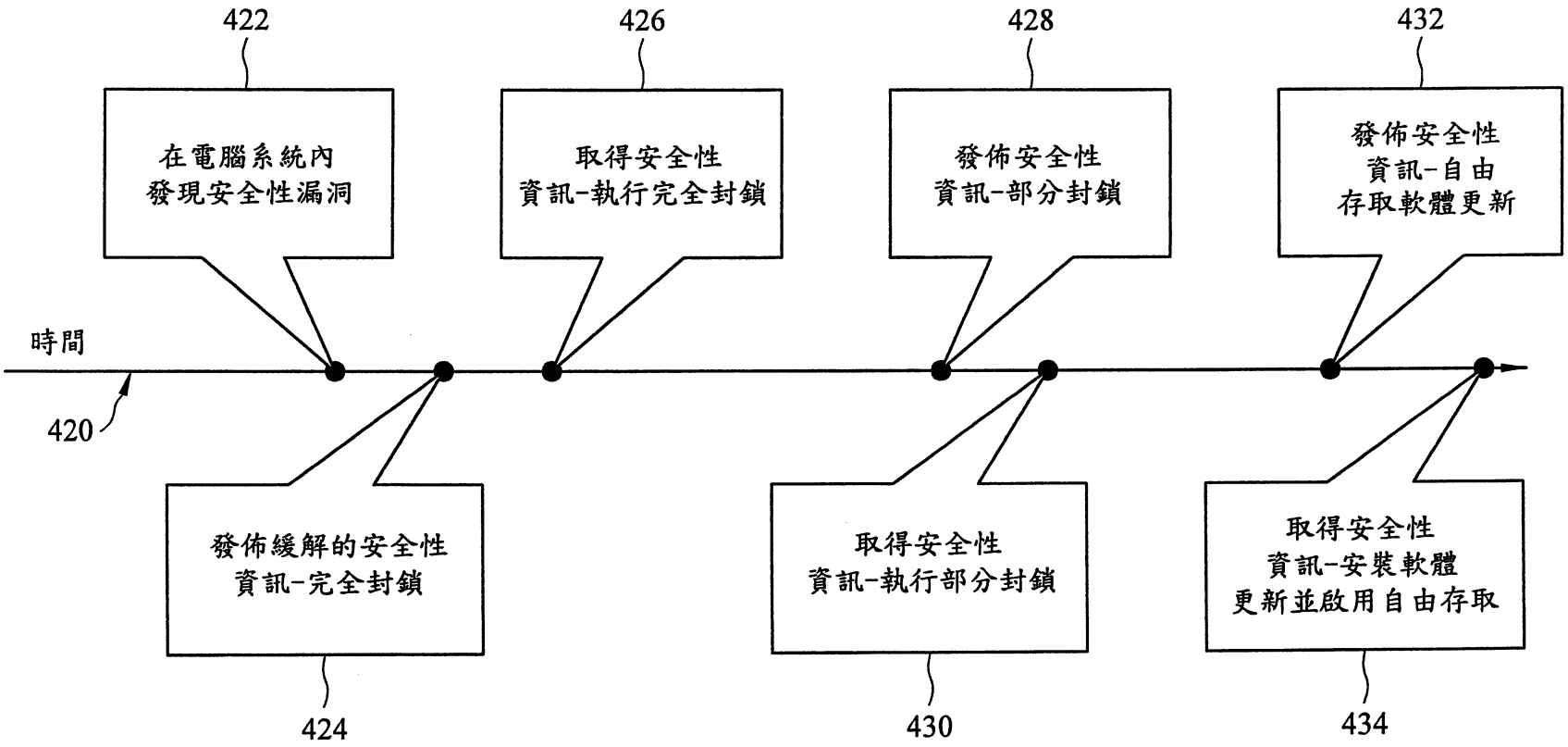
第 3B 圖

200529002

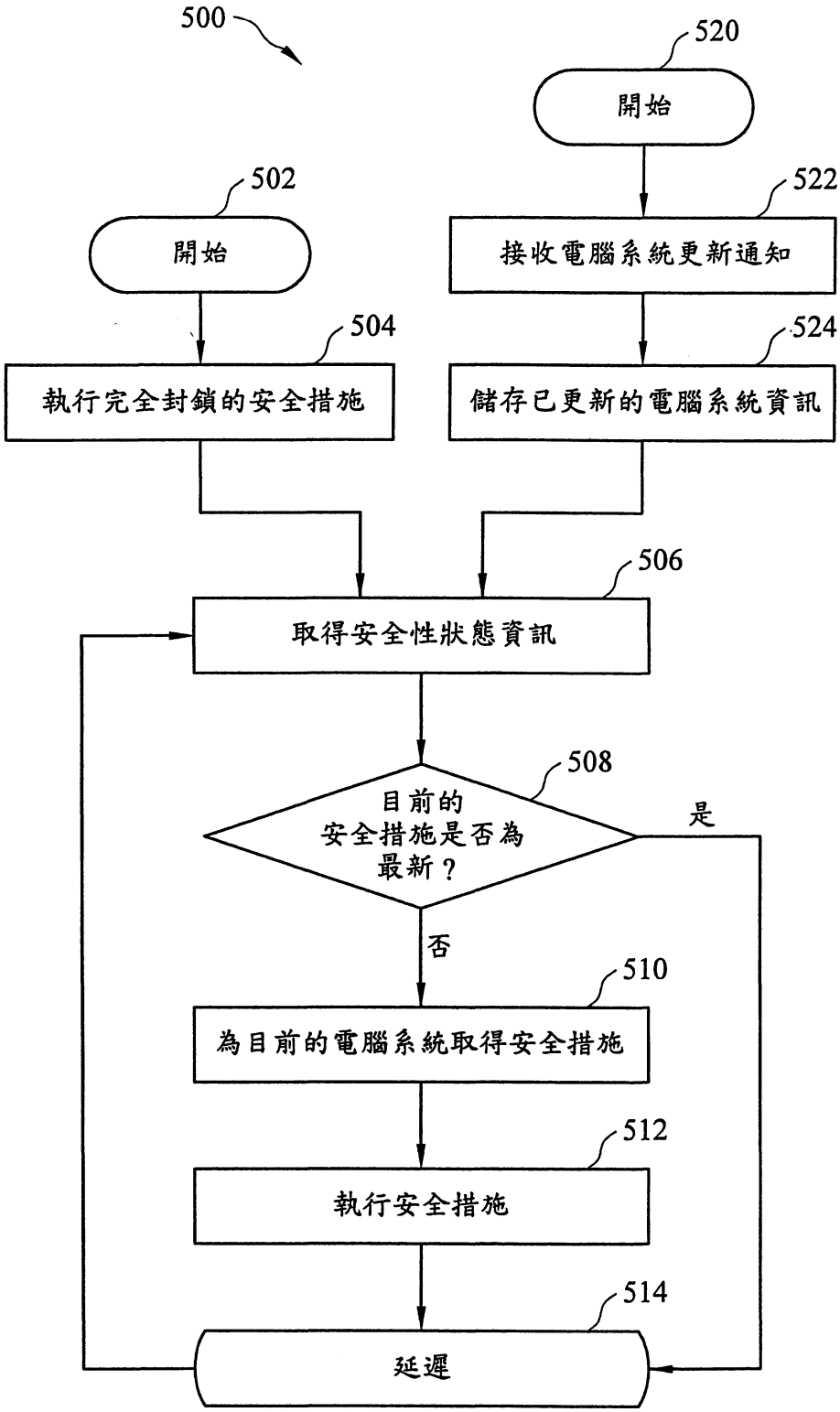


第4A圖

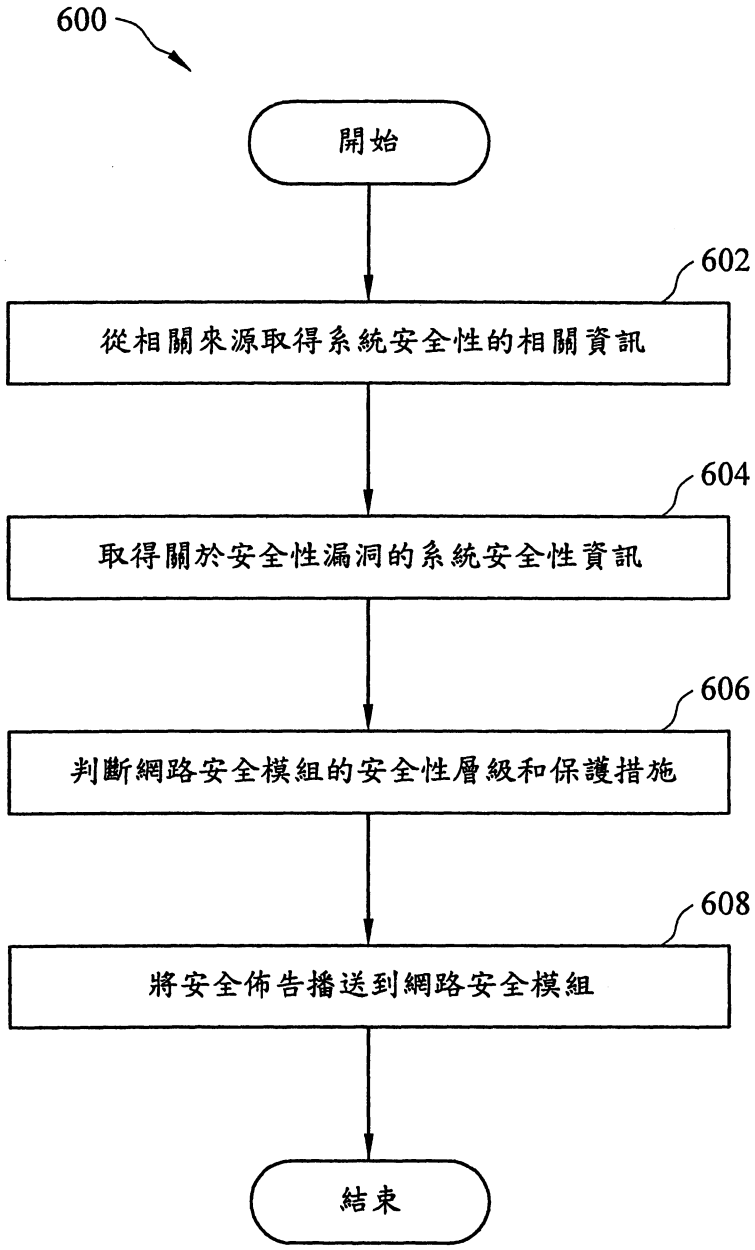
200529002



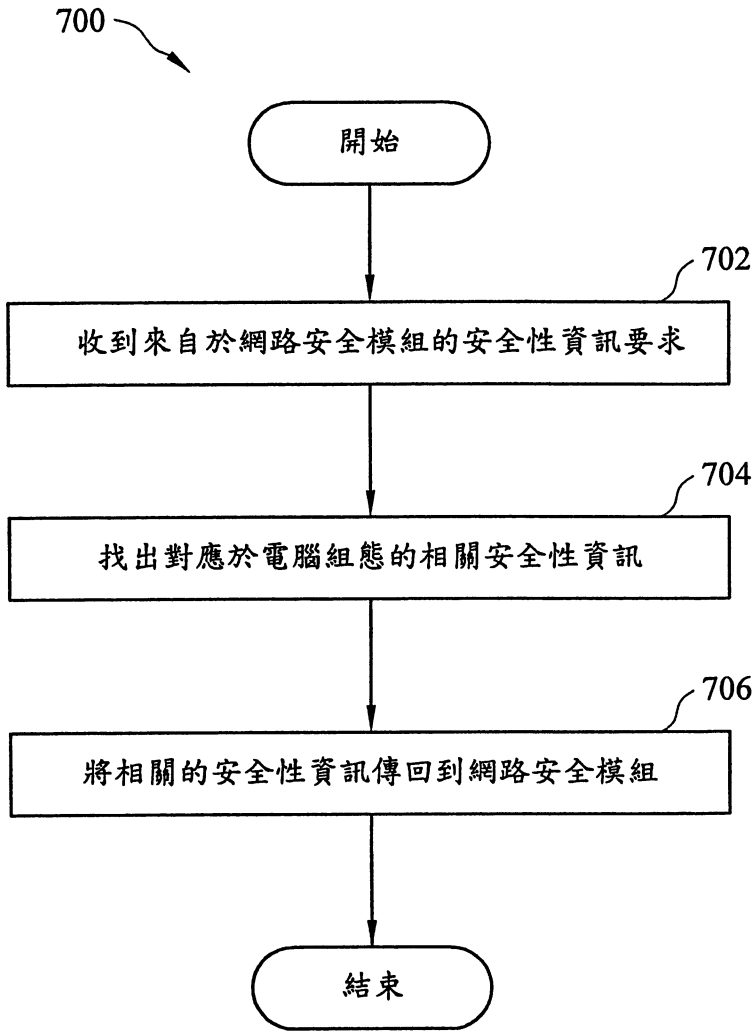
第 4B 圖


500
520
開始
502
522
開始
接收電腦系統更新通知
504
524
執行完全封鎖的安全措施
儲存已更新的電腦系統資訊
506
取得安全性狀態資訊
508
目前的
安全措施是否為
最新？
是
否
510
為目前的電腦系統取得安全措施
512
執行安全措施
514
延遲

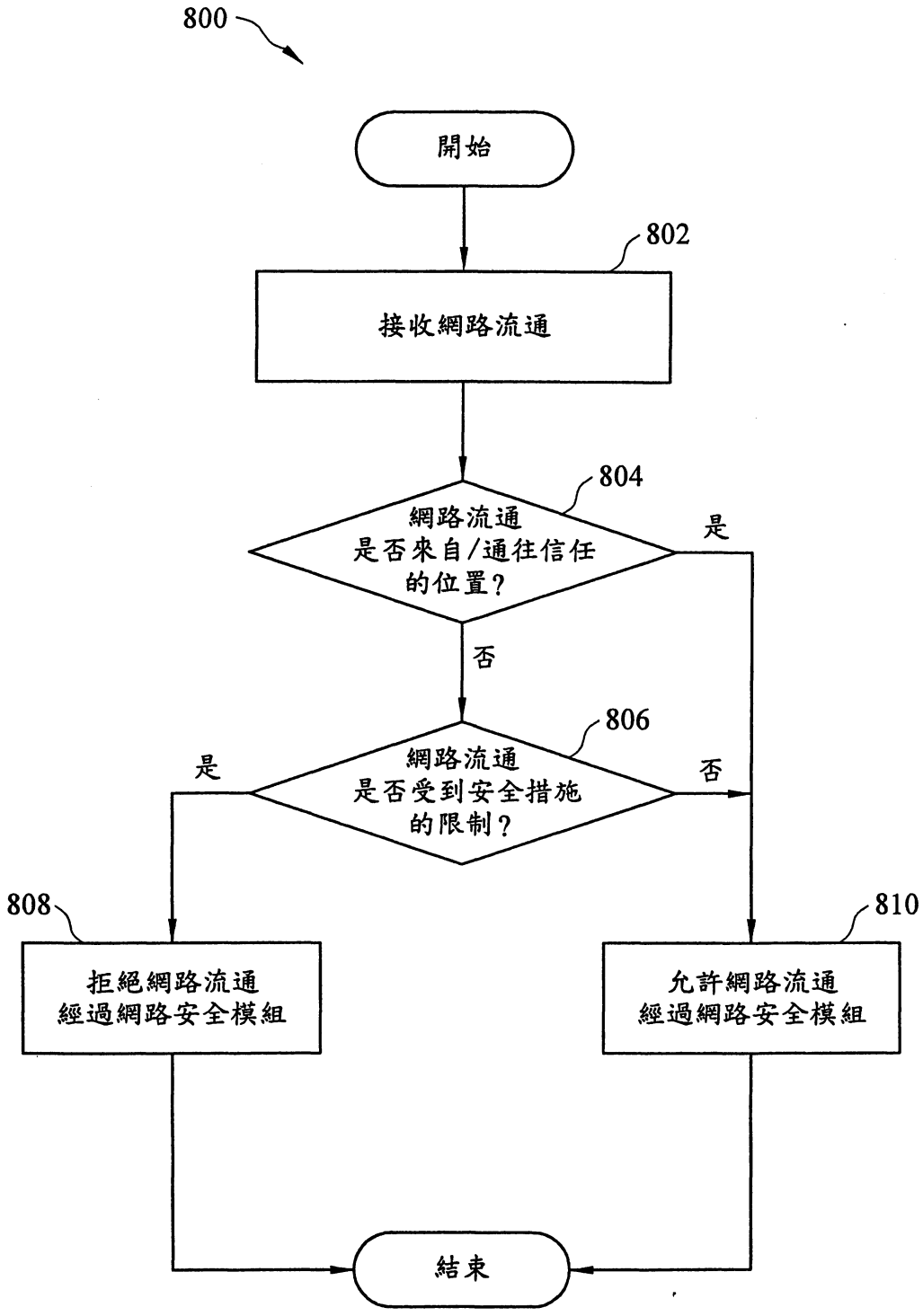
第 5 圖


600
開始
602
從相關來源取得系統安全性的相關資訊
604
取得關於安全性漏洞的系統安全性資訊
606
判斷網路安全模組的安全性層級和保護措施
608
將安全佈告播送到網路安全模組
結束

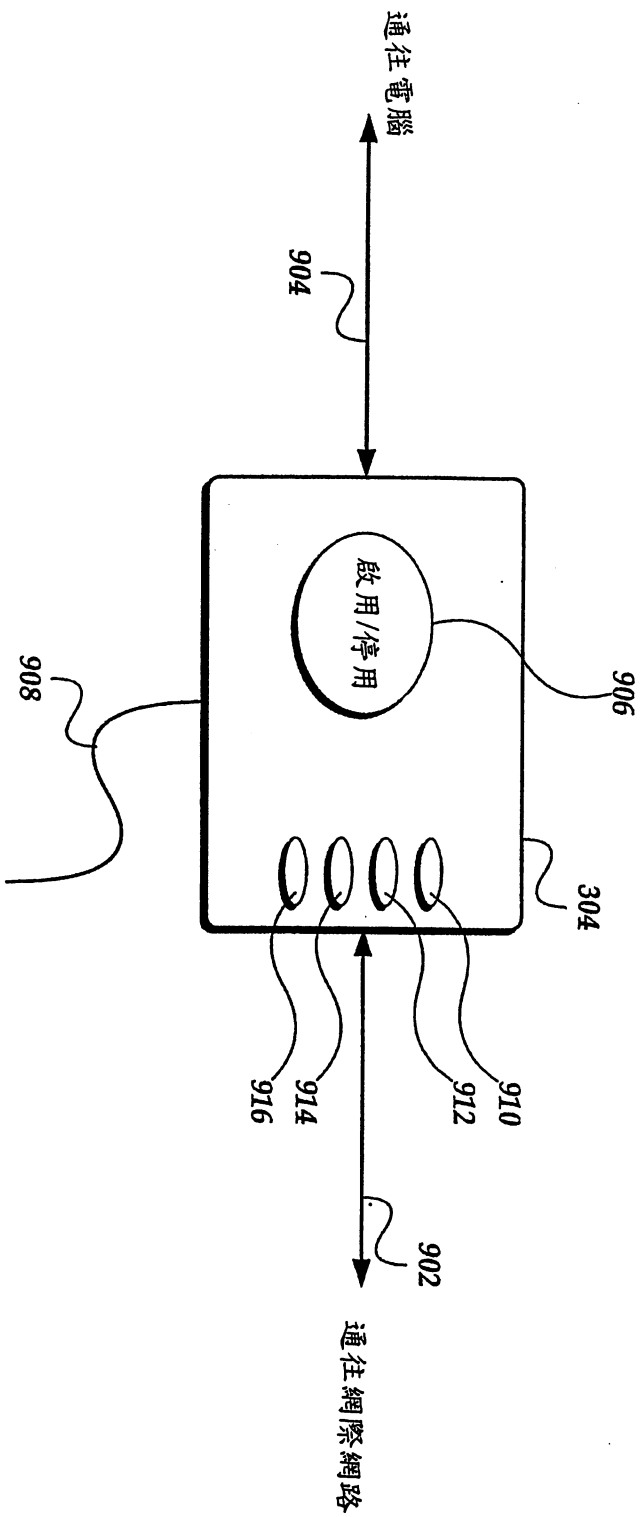
第 6 圖


700
開始
702
收到來自於網路安全模組的安全性資訊要求
704
找出對應於電腦組態的相關安全性資訊
706
將相關的安全性資訊傳回到網路安全模組
結束

第 7 圖

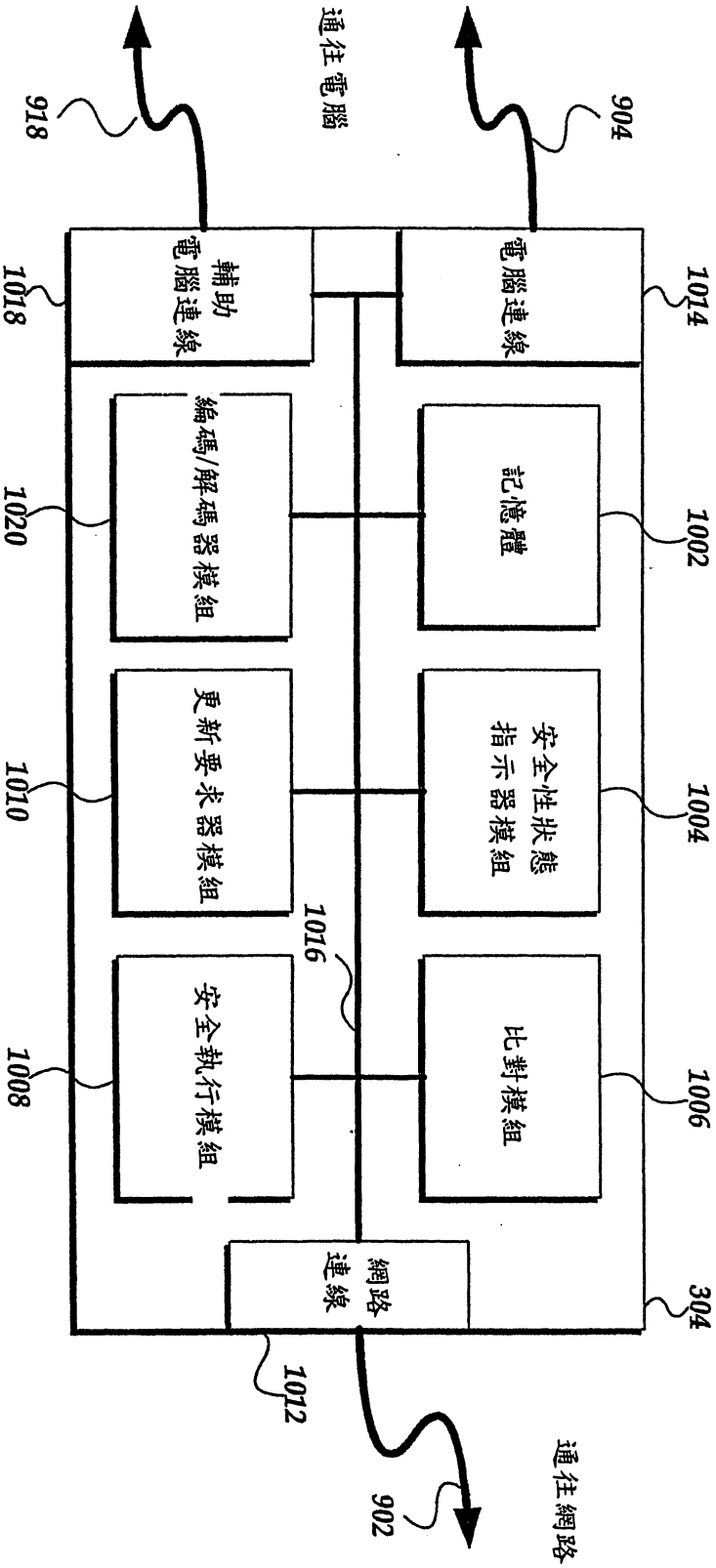

800
開始
802
接收網路流通
804
網路流通
是否來自/通往信任
的位置？
是
否
806
網路流通
是否受到安全措施
的限制？
是
否
808
拒絕網路流通
經過網路安全模組
810
允許網路流通
經過網路安全模組
結束

第 8 圖

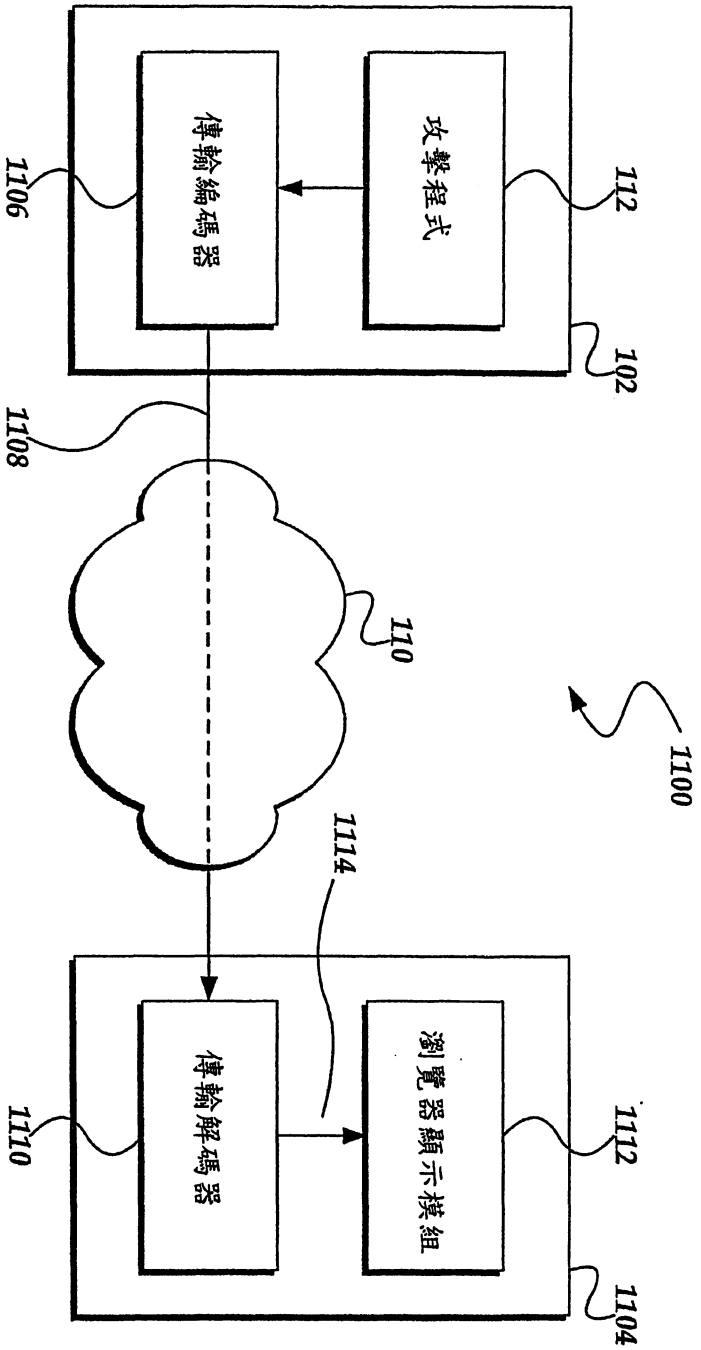


第 9 圖

200529002

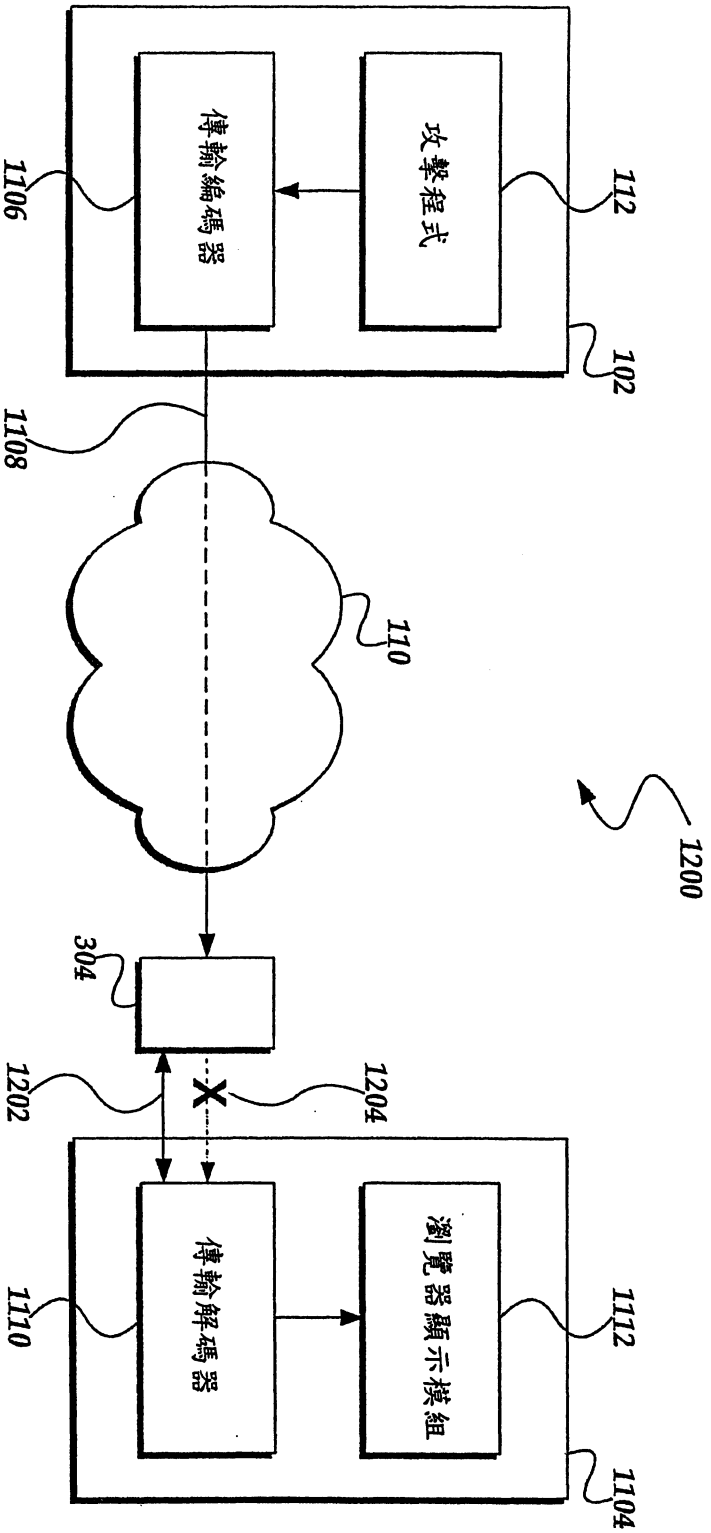


第 10 圖

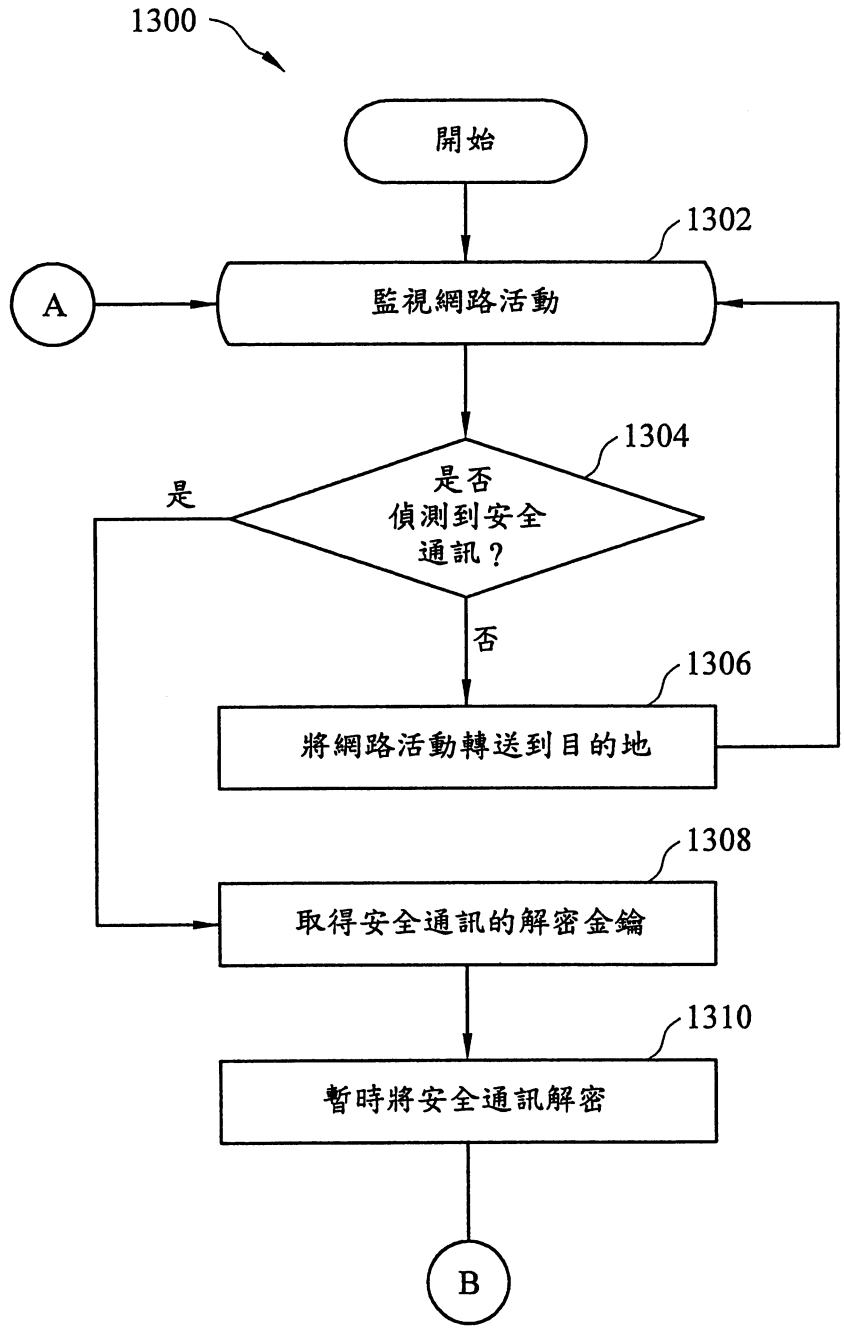

攻擊程式
傳輸編碼器
112
1106
102
1108
110
1100
1114
傳輸解碼器
瀏覽器顯示模組
1110
1112
1104

第 11 圖

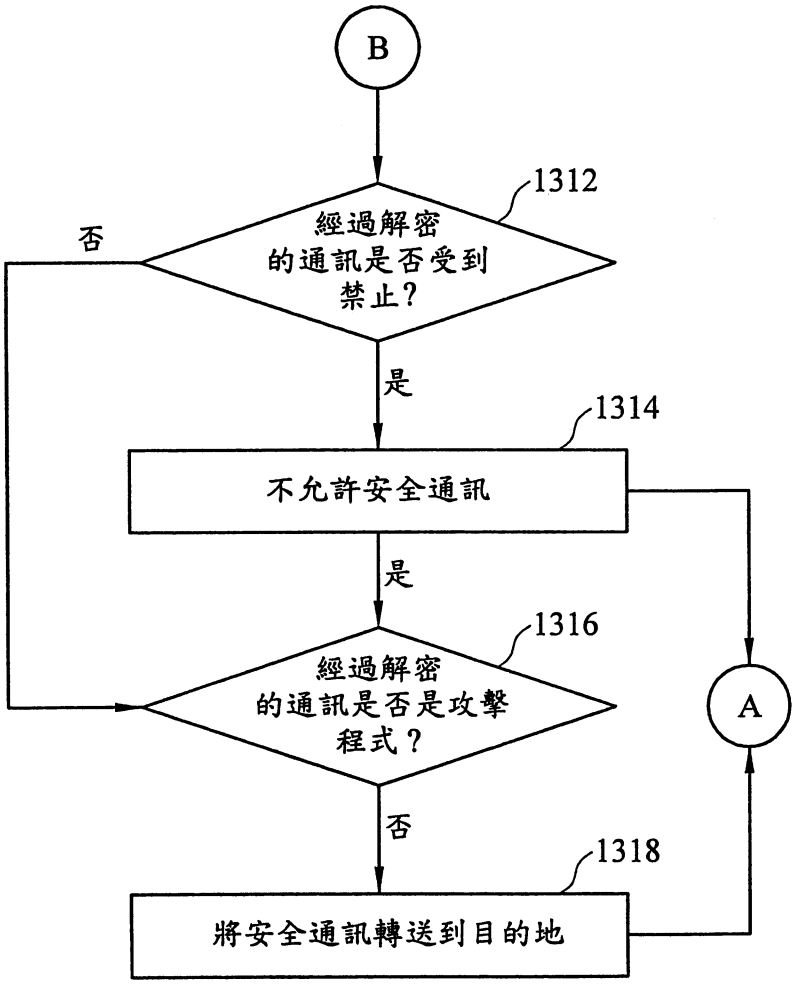
200529002



第 12 圖


1300
開始
1302
A
監視網路活動
1304
是否
偵測到安全
通訊？
是
否
1306
將網路活動轉送到目的地
1308
取得安全通訊的解密金鑰
1310
暫時將安全通訊解密
B

第13A 圖


B
1312
經過解密
的通訊是否受到
禁止?
否
是
1314
不允許安全通訊
是
1316
經過解密
的通訊是否是攻擊
程式?
否
1318
將安全通訊轉送到目的地
A

第13B 圖

柒、指定代表圖：

(一)、本案指定代表圖為：第 12 圖。

(二)、本代表圖之元件代表符號簡單說明：

102 電腦

110 通訊網路

112 電腦攻擊程式

304 網路安全模組

1104 計算裝置

1106 傳輸編碼器

1110 傳輸解碼器模組

1112 瀏覽器顯示模組

1200 示範性環境

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無