行政院國家科學委員會專題研究計畫成果報告

計畫編號：NSC 91-2213-E-009-084
執行期限：91 年 08 月 01 日 至 92 年 07 月 31 日
主持人：葉義雄
執行機構及單位名稱：國立交通大學資訊工程學系

The Design and Implementation of Intrusion Detection on Mobile Agent

壹、 中英文摘要

摘要:

隨著網際網路的普及、行動通訊技術的成熟與軟體技術的演進，在不久的未來透過行動通訊設備所能提供的頻寬將不再只適合傳遞聲音更能運用於資訊的傳遞，而且相關運算設備上所承載的程式將不再只是侷限於在同一硬體設備上完成所需完成的任務，程式將可隨需要在不同硬體環境間漫遊，更可透過網路通訊達到分進合擊的效果，如此便利的運算環境不僅讓人類可透過行動通訊技術任意移動運算環境硬體設備的地理位置，更可讓程式與相關運算資料隨意遊走，這無疑的也提供了一個更便利的入侵環境與及更複雜的攻擊行為，因此如何偵測此一複雜的攻擊與入侵行為是影響推展行動計算環境成敗的關鍵技術。

本計畫將著重於探討行動代理人相關的安全問題，著重於代理人與網際網路環境對攻擊與入侵行為可能模式作深入探討並以此設計相關的入侵偵測系統與相關安全性規範以避免及抵抗未來此一環境所可能遭受的惡意攻擊。

關鍵詞：行動代理人、入侵偵測系統、網路安全及行動通訊

Abstract

By internet growing, mobile communication and software technology developing, in predicted future the bandwidth of the communication device is not only for voice but also information transformation. The program is not restricted in the device. It may route between different hardware devices to complete jobs by network. It provides mobile computation environment for people to avoid restrictions on fixed places. In the mobile environment, all the information moves around, it exactly provides a convenient environment for more novel and complicated attack behavior. Thus, intrusion detection is an important article in developing mobile computing environment.

The project focuses on the security issues within mobile agent platform, especially in the possible intrusion behaviors of mobile agent. Further we design an intrusion diction system and related security policies which is successful to resist some possible attacks theoretically.

Keywords：Mobile Agent、Intrusion Detection、Network Security and Mobil Communication.

貳、 緣由與目的

安全上的威脅通常可分為三大類：

1. 資料的暴露。
2. 禁止電腦的某些服務或使其無故當機。
3. 資料的訛用、訛誤。

當對代理程式申請服務時有多種詳細的方法可檢測針對上述的三大安全性的威脅，我們以代理程式的組成元件來對上述威脅分類並用以確認攻擊可能的來源地與目的地。值得注意的一點是上述的很多威脅在過去Client-Server架構的系統中也是存在的（執行來源不明的程式，如經由網路下載或磁片），只是在mobile agent的架構下威脅性變大了。

有很多種模組可用來描述代理系統，然而針對安全性問題的考量時採用一種最簡單的一種模組，主要包含有代理系統與代理系統作業平臺的模組便已經足夠。

本計畫將針對如何規劃與設計一個行動通訊環境之行動代理人入侵偵測系統，並結合相關行動通訊技術、網路安全技術、行動代理人技術與入侵偵測技術，以提供未來行動通訊環境伊抵抗與偵測可能跨平台的入侵與攻擊行為。以提升行動通訊環境的安全強度。

因為行動通訊技術的演進與行動代理人技術的運用須有相關的安全機制與防禦機制配合，唯有如此行動通訊技術與行動代理人技術才能提供相對可靠與安全的計算與通訊環境，如此才能提供一可行的行動通訊環境建立之遠景。

參、 研究結果與討論

一、 Study on mobile agent

1. Mobile agent:

所謂的代理程式包括要完成計算所需要的程式碼和執行狀態，而所謂的行動代理程式是指允許代理程式由在各個不同代理系統作業平臺之間遷移並執行。

2. Mobile agent platform:

而所謂的agent platform需能夠提供agent一個作業環境使agent能在其上進行操作，並能滿足agent所提出的服務要求。在mobile agent架構中，agent在其執行過程中可能會經歷很多個platform，其中一開始的那個通常被稱為home platform，他與agent有最密切的關係(agent可能是從此地發展的)，其後隨這遷移的次數的增加使的整個關係越來越複雜，安全上的威脅也越來越多。

3. Agent-to-Platform attack：

偽裝、假冒(Masquerading)

所謂的偽裝或假冒是指一個未經

受授權的代理程式對其他的（合法）代理程式提出要求。偽裝、假冒者通常會假扮成已授權的代理程式以便獲得存取其未經授權的服務或資源，假冒者也有可能會假冒成另一個未經授權的代理程式並藉此來轉移那些因為其假冒行為而可能遭受的責備。一個偽裝、假冒的代理程式可能會破壞的合法的代理程式彼此之間的信任或相關的名譽。

拒絕服務、阻斷服務攻擊(Denial of Service)

行動代理程式可經由大量佔用代理程式作業平臺執行計算所需的資源而進行阻斷服務攻擊阻斷服務攻擊也可能經由執行具攻擊性的程式碼故意性的攻擊系統弱點或利用程式的錯誤。

在mobile agent的架構下platform通常需執行一些外來的agent的程式碼，這是危險的，假如說在執行前沒有做好事先的檢查。一個懷有惡意的agent可能會帶來具有破壞性的程式碼（如病毒），攻擊platform 造成platform的效率降低，隨這攻擊程度的不同有造成的傷害也不同（如效率降低、platform的結束甚至於是整台電腦的當機都有可能）。

未授權存取(Unauthorized Access)

存取控制的機制是用來預防未經授權的使用者或程式存取（使用）其不該（未經授權）使用的服務或資源。當一個agent新抵達一個 agent platform時就需遵守platform的安全規定，為了實現適當的存取控制機制通常換要求platform在一開始就必須先確認mobile agent的身份。

一個未經允許存取platform和其提攻的服務會造成對platform和其他agent的傷害，因此platform必須確保agent不會去存取那些不該（未經授權）存取的資料（包括存在catch中或是臨時儲存體中的所有資料）。

肆、 Study on Intrusion Detection :

什麼是入侵行為? 什麼是入侵偵測?入侵行為即為有人想要破壞或濫用你的系統,其中入侵的行為可能是竊取機密的資料或是盜用一些網路的服務:如 e-mail FTP service 等等。

入侵偵測即為找出入侵的行為，並加以處理，主要為收集使用者和攻擊者的行為，並分析這些行為的模式，藉由這些收集的資料，使得入侵偵測系統可以判斷出哪些行為是入侵的行為，藉此偵測出可疑的入侵或誤用動作，並於偵測到入侵的行為時，能夠對管理者發出警告或使安全機制做出反應，使得損害達到最小。

入侵偵測系統之偵測方式

偵測方式可分「監督網路作用(network-based)」與「監督系統

(host-based)」兩種。

監督網路運作的入侵偵測系統會在網路上的節點放置一各監控裝置，基本上是一種網路監聽程式，它會接受所有經過其監聽設備的網路通訊，分析其中的內容：如來源、目的、使用的網路運用等傳輸內容。並可從中判讀可疑的攻擊動作或誤用情形。

監督系統運作型式的入侵偵測系統，主要放置在主機上，可以監控所有在主機上使用者行為與作業系統的動作，如 : 系統安全性掃描、安全性漏洞資訊的、監督系統上的重要檔案存取、是否有監聽程式、系統程式是否被更動等，來判斷其監督的系統上是否有可疑入侵者。

伍、 結果與討論 :

本次入侵偵測系統的做法是先採用監督系統(host-based)的機制，利用將它架設在 mobile agent platform 的平台上，以偵測當 mobile agent 在它所在 mobile agent platform 上所做的一些行為，在以 host-based 系統為機制下，對於 agent 在 agent platform 上所做的行為偵測採用的策略是「規則比對(rule-base)」，這同時也是目前在入侵偵測上最常見的實現方法，藉由定義一些最常見的入侵行為，當 agent 一但進入 agent platform 的系統中，它所做的一些存取行為會由事先存在入侵偵測系統所定義的行為模式作比對，以判別所做的存取動作是否合乎標準，這些行為例如：是否有掃描所有的 port、是否在一直重複作 password re-try 的動作，為了能夠猜中密碼進而取得更高的存取權限等；當然對於 agent 的行為比對也是花系統不小的負擔，所以在比較的模式上先將其略分為兩部分作為不同層級在不同時間的比較，在確切的環境作比較適合的異常行為比較策略，例如，將相對於系統異常行為的比對 agent 分成未授權和已授權兩種，在未授權 agent 的行為異常比對上，可以定義像是企圖存取合法授權 agent platform 的資源，或是未授權的 agent 正在掃描授權(合法) agent platform 的 port，以便系統偵測到時即時發出相對應的警訊；另外，經由 agent platform 已認證後而進入系統後的 agent，也有可能因為 agent 本身的程式碼寫作的不當造成對系統的濫用，例如：不斷的送出請求服務的要求系統作服務，造成系統一直只作你的服務，不當 agent platform 資源的存取、干擾 agent 和 platform 或是 agent 和 agent 之間的溝通等，所以在經系統認證後的 agent，它在系統裡行為比較的行為模式上又可分為:agent 對 agent 的行為和 agent 對 agent platform 之間互動的行為比較；將異常行為的比較策略依照不同的環境對 agent 行為作比較，不只使管理有調理化，也可使的系統不會每次因為 agent 作 access 時，而無條件的全部去比對先前所定義的所有行為，可以使的系統減少一

些負擔。

陸、 未來發展方向

未來希望能夠將「規則比對(rule-base)」的機制，能夠改換成自動學習的異常行為的比對，這也是目前入侵偵測最熱門的技術，因為入侵的手法時常在變化，使的異常比對行為的 rule 會越訂越多，若是能從每次入侵手法中學取經驗，可以防止之後以相同入侵手法的變形，這樣的機制被建立，則系統以後的安全部會讓管理者花太大的心思去處理，這也是目前我們正極力去學習的目標。

柒、 參考文獻

[01]L. Hagen, J. Mauersberger and C. Weckerle, Mobile agent based service subscription and customization using the UMTS virtual home environment, Computer Networks 31 (19) (1999) pp. 2063-2078

[02]Menelaos K. Perdikeas, Fotis G. Chatzipapadopoulos, Iakovos S. Venieris and Gennaro Marino, Mobile agent standards and available platforms, Computer Networks 31 (19) (1999) pp. 1999-2016

[03]Claudia Raibulet and Claudio Demartini, Mobile agent technology for the management of distributed systems – a case study, Computer Networks 34 (6) (2000) pp. 823-830

[04]Richard Feiertag et al., Intrusion detection inter-component adaptive negotiation, Computer Networks 34 (4) (2000) pp. 605-621

[05]Peter Sommer, Intrusion detection systems as evidence, Computer Networks 31 (23-24) (1999) pp. 2477-2487

[06]Marc Dacier and Kathleen Jackson, Intrusion detection, Computer Networks 31 (23-24) (1999) pp. 2433-2434

[07]Ming-Yuh Huang, Robert J. Jasper and Thomas M. Wicks, A large scale distributed intrusion detection framework based on attack strategy analysis, Computer Networks 31 (23-24) (1999) pp. 2465-2475

[08]Peter Sommer, Intrusion detection systems as evidence, Computer Networks 31 (23-24) (1999) pp. 2477-2487

[09]Steve Mott, The second generation of digital commerce solutions, Computer Networks 32 (6) (2000) pp. 669-683

[10]Marc Dacier and Kathleen Jackson, Intrusion detection, Computer Networks 31 (23-24) (1999) pp. 2433-2434