透過封包監聽分析偵測 IP-MAC 位址盜用行為

蘇建郡　范聖緯
南台科技大學資訊管理研究所
台南縣、台灣
ccsu@mail.stut.edu.tw　m9790226@webmail.stut.edu.tw

摘要

在網際網路如此發達的現代，網路管理一直是重要的課題，如何適當的調配網路資源、防範、發現網路上惡意的行為是每位網管人員努力的目標。網路上許多的惡意行為不斷的推陳出新，有的惡意行為，必須要搭配昂貴的設備、複雜的管理系統，才能有效控制。本論文針對其中一項不易解決的問題:IP-MAC 冒用，提出一個不依靠交換器 Port 鎖定，只利用封包監聽，配合簡易的資料庫系統，從網路上傳送的未加密封包中擷取出各主機瀏覽器之 User-agent、防毒軟體識別碼、即時通訊軟體帳號、電腦名稱，來達到主機辨識的功能。

關鍵字: IP-MAC 冒用, 封包監聽 , 主機辨識

I. 前言

現今網際網路已非常的普及，不論在政府機關、各級學校、私人組織等，都有許多的使用者在工作上、生活上都無法離開網路。每個組織內部的使用者數量、習性、所擁有的網路資源皆不相同，因此，如何將現有的網路資源妥善的分配至所管轄區域，並依情況作適度的調整，讓區域內的使用者們都能滿意的使用網際網路一直是網路管理者在研究的課題。

網路管理者們大多會使用一套特別的系統，讓管理者能夠掌握所管轄區域內的網路使用狀況，分析流量、使用者是否合法等，找出異常，再搭配網路設備本身具有的過濾、管理功能，對這些異常使用者作出處置，維持網路效能[1]，其系統大多是透過網路卡之 MAC(Media Access Control)位址與 IP 位址綁定進行識別使用者的工作。但隨著 Windows XP 系統之風行，其系統本身便能讓使用者進行 MAC 位址的更改[2]，讓惡意的使用者能有機會去冒充為其他的使用者，盜用其資源，造成網路管理上的盲點, 目前常見之對應方法，多為透過交換器的 Port 資訊，來對 MAC 位址進行紀錄、鎖定等[3]。但此種方法須購買有支援此功能之交換器，當所管理的網路範圍越大，其所需付出的設備成本，管理的複雜度，都會不斷的增加。

本論文透過擷取網路上傳遞的封包，解析後將使用者端主機的各項特徵存入資料庫中，並利用這些特徵值來判斷使用著主機目前所使用的 MAC 位址是否經過了更改，來達到不需使用交換器上 Port 資訊，就能辨識出 MAC 位址是否遭到了惡意的竄改、冒用，幫助網路管理者在低成本的情況下，就能作出正確的判斷。

II. 研究背景

A. MAC 位址(Media Access Control):

在乙太網路中，封包的傳遞並不依靠 IP 位址，而是依靠網路設備上出廠時已設定好的 MAC 位址來決定封包由哪個設備來接收。MAC 位址共 48 位元（6 個位元組），以十六進位表示， 例如:00：06：30：AA：BB：CC。前面 24 位元由硬體廠商自行決定，後 24 位元由 IEEE (電機電子工程師學會 , Institute of Electrical and Electronics Engineers) 等各組織決定如何分配。在正常情況下，每個 MAC 位址在世界上都是獨一無二的，但近年作業系統的演進，在軟體上並未特別將 MAC 位址鎖定，讓使用者有機會自行更改 MAC 位址，去達到特殊的目的，造成網路管理上的問題。

B. 基礎網路管理系統

以全國各大學為例，現今網際網路在校園中的應用非常的廣泛、學生們利用網路選課、上傳作業、教師利用網路教學、點名、收發 Mail 等，各式各樣的網路系統都出現在各大專院校之中，在校園中所有的人都會使用到。但網路資源並不是無限的，必須適當的分配網路資源，避免如:P2P、網路病毒、網路遊戲等造成網路資源遭到佔用的異常狀態，在各校園皆有其用來控管網路資源的系統。

由於各大專院校其本身擁有的資源皆不相同，其系統的功能也不盡相同，但最基本的，大多都是紀錄使用者 MAC 位址後，再配給 IP 位址，並觀察此 IP-MAC 配對是否有超出限制的流量[4], 如圖 1

圖 1.　基礎網路管理系統

當某個 IP-MAC 配對使用的流量超過了系統的上限之後，便會對使用此 IP-MAC 配對加以阻檔，禁止其使用網路。此種管制方法，的確能避免未註冊的使用者使用網路，也能防止少數的使用者持續不斷的下載各樣的資料，影響到整體網路的效能。但此種管理方式的缺點，就是無法分辨出 IP-MAC 配對整個被冒用的情況。

C. Port Security

為了避免 IP-MAC 配對同時遭到了冒用，大部份的網路管理者都會採取 MAC 位址與交換器 Port 鎖定的方式，讓註冊過的 MAC 位址只能在固定的交換器 Port 上使用，當有冒用者出現時，雖然他成功的冒用了 IP-MAC 配對，但無法通過交換器的過濾，的確能防止冒用，但此種方法仍有其缺點，尤其是管理區域越大時，缺點就越明顯。

1) 管理不易:當有使用者要離開、或更換工作場所時，就必須要登入交換器的管理介面，進行 MAC 位址的修改，當管理範圍小時，還可接受，但範圍慢慢加大時，就會造成管理者很大的負擔。

2) 無法掌握運作情形:以校園網路為例，當校內的系所處室等數量眾多、校地廣大之時，要作到 MAC 位址鎖定就必須要掌握到各系所處室所擁有的網路設備有哪些，分佈在哪一層樓、哪一間辦公室，網路線是如何佈線的。在一些歷史悠久近年才慢慢導入網際網路的學校根本作不到，系所處室可能在開始導入設備時，就缺乏與網路管理者的良好配合。如圖 2:

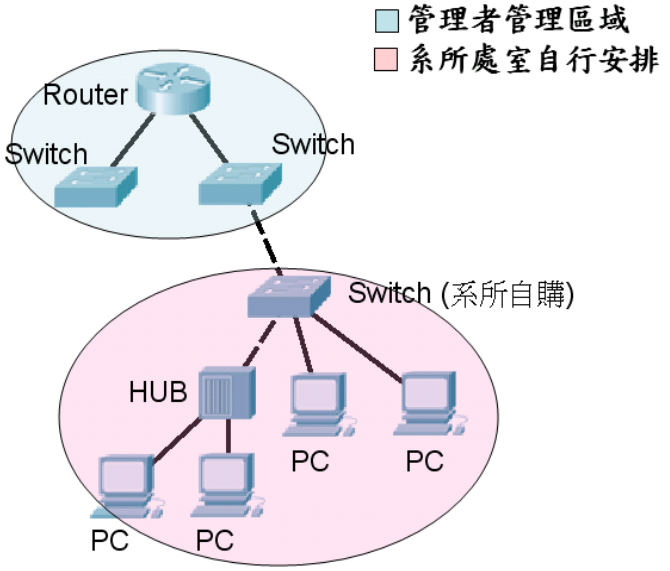

圖 2. 缺乏良好規劃的校園網路

但當某個 IP-MAC 配對遭到冒用導致禁權後，系所處室仍會前來尋求網路管理者之幫助，造成管理者在排除問題上仍要花費許多的時間，甚至無法找出冒用者是從何處連上網路，於是本論文試著實作一個系統，讓 IP-MAC 配對遭到冒用後，能在損害發生前察覺，進而找出冒用者。

III. 系統架構

本研究利用 Wipacp 函式庫與 VC++開發出一套運作在 Win32 平台下的網路封包擷取軟體，並將擷取的封包進行解析，將所需要的特徵值存入 MySQL 中，供日後擷取到相同類型之封包時，進行新舊資料的比對，來找出異常。目前監控的環境皆為採用 Win32 平台的作業系統。

A. 使用元件

1) ***Winpacp:***

全名為 **Windows packet capture**，是一個運行在 **Win32** 平台下的免費函式庫，讓 **Win32** 平台下的應用程式能夠有讀取網路底層(如實體層、鏈結層)資訊的能力。主要能夠作到抓取數據封包、透過自訂條件過濾數據包、產生簡易的封包、統計流量等功能。本研究主要使用其抓取封包的功能。

2) ***MySQL:***

是一套歷史悠久的網路資料庫系統，具備有誇平台、多執行緒、多使用者、免費、執行速度快等特性，受到許多開放源碼的系統的使用。本研究主要使用其來儲存網路封包解析出的使用著特徵值，並紀錄使用者的其他行為。

3) ***使用者特徵:***

來源為網路使用者在正常使用網路的情況下，取出其傳送的封包中未加密且與使用者特性、主機識別有關的資訊，來達到不讓使用者發覺的情況下，就能識別其使用的主機有無變化。目前系統主要抓取下面四項特徵。

- **使用者代理(User-agent):** 在瀏覽網頁時，會傳送許多標頭至 Web 伺服器，讓伺服器決定如何回應，使用者代理為其中一種標頭，其中帶有瀏覽器的名稱、版本、作業系統等資訊[5]。
- **電腦名稱:**指的是 **Win32** 平台在區域網路上的電腦識別名稱，讓區網內的電腦都能順利識別彼此，主要利用微軟的 **SMB** 協定進行傳輸[6]。值得注意的是此協定完全在區網的架構運作，如監測的對像在不同的區網，就需對連接不同區網間的網路設備進行 **Mirror** 設定。
- **防毒軟體名稱、識別碼:**現今網路安全一直是受到注重的議題，幾乎所有擁有上網功能的主機都會安裝防毒軟體來達到基本的防護，這些防毒在更新時，其封包中都會帶有其軟體名稱及用戶的驗證碼，讓更新伺服器可以判斷其是否為合法授權的使用。如: **Kaspersky**、**Avira AntiVir Personal**、**Norton** 等皆有此特性。
- **即時通訊軟體:**在現今網路網路風行的即時通訊軟體如 **MSN**、**YAHOO** 即時通等，都需使用帳號密碼登入，而在登入過程中，其中帳號資訊皆是明碼未加密，只有密碼會加密，此資訊可以用來識別使用者的身份。

B. 系統架構

本研究開發的系統主要有三個部份

1) ***特徵值比較部份:***

在資料庫中，對每一個特徵值設定了欄位如表 1:

表 1. 特徵值欄位格式

現有特徵	最後出現時間	暫存特徵	最初出現時間

- **現有特徵:** 當系統開始運作，初次截取到的特徵。
- **最後出現時間:** 現有特徵最後的出現時間，格式為年、月、日、時。
- **暫存特徵:**當系統開始後，在同樣的 IP-MAC 配對上所出現與現有資料特徵的紀錄相異的特徵值。為

了避免是正常的更新(如:IE6 升為 IE7)，先行紀錄下來。

- **最初出現時間:**暫存特徵值的最初出現時間，格式與最後出現時間相同。

本研究設計了一套流程，來紀錄某個 IP-MAC 配對所在主機的 4 個特徵值並判斷其變化是否屬於冒用還是正常的更新，如圖 3。當特徵值發生了變化後，會存至暫存特徵欄位。當某個 IP-MAC 配對特徵值發生變化的個數越多，就越有可能是遭到了冒用。如果只有一個特徵值發生變化，此暫存特徵也已出現了一段時間，現有特徵值在這段時間內也沒有出現，就可以判斷為正常的更新。暫存特徵出現多久後才該視為安全，則要依據所監測的區域內使用者的習慣來決定，故此先用 N 小時來表示，如果常有冒用情形，此安全時間的設定就應拉長，反之則縮短。

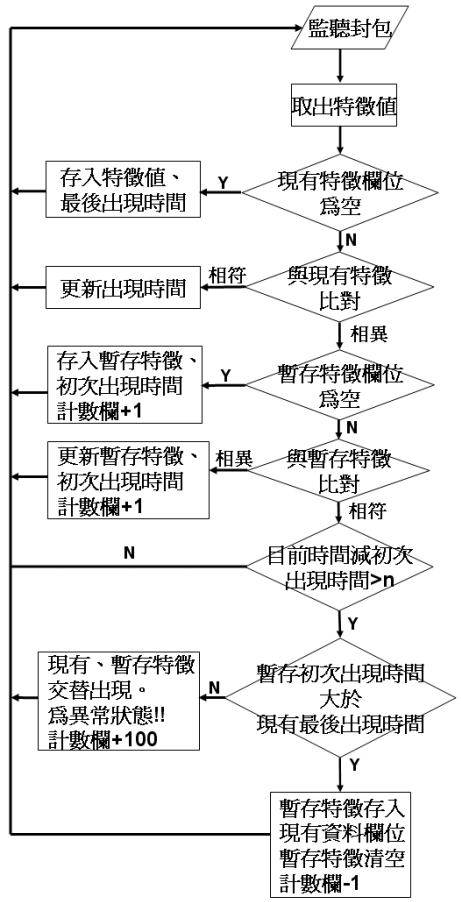

圖 3. 特徵值判斷流程

2) 使用者瀏覽紀錄:

當使用者開啟一個網頁後，Http 協定會使用 GET 要求向 Web 伺服器要求檔案，譬如顯示一個完整網頁所需用到的圖片等。本系統會紀錄有 GET 動作且次數超過 18 的封包目的位址，來了解某個 IP-MAC 配對的網路使用習慣。次數基準是以 Google 首頁為例[7]，開啟一次 Google 首頁會發生約 6 次 GET，本系統取其 3 倍為基準，當大於 18 次，系統就會認為這是個有效的紀錄，此舉主要是為了過濾一些廣告圖像性質的 GET，它們容易隨著網頁的重新整理而發生變化，向不同的目的位址取回廣告圖像，這樣少量多變的目的位址並無法有效的判斷瀏覽習慣。對每個 IP-MAC 配對皆分為兩個資料庫，暫存的、歷史的資料庫，皆有相同的欄位如表 2。當系統透過 SMB 協定發覺關機或異常時，便會對瀏覽紀錄進行處理，流程如圖 4

表 2. 瀏覽紀錄欄位格式

Dest	Times

- **Dest:**使用者所瀏覽的網頁 IP 位址。
- **Times:**此 IP 位址發生 GET 的次數。

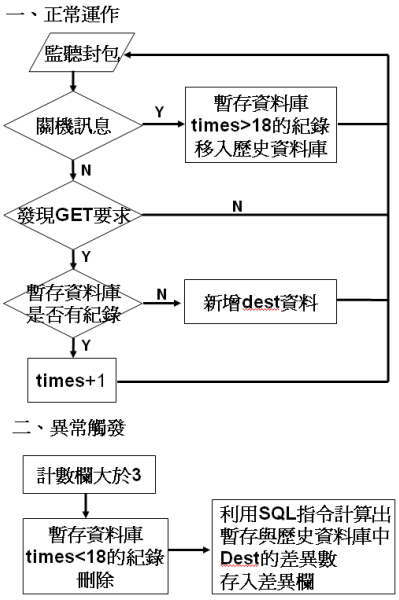

圖 4. 瀏覽紀綠運作流程

3) 結果顯示欄位:

表 3. 結果顯示欄位格式

差異欄	重覆欄	計數欄

- **差異欄**：顯示目前此 IP-MAC 配對的瀏覽紀錄與歷史資料庫中的差異數，差異數越多，代表此使用者的行為模式改變的越明顯。
- **重覆欄**：暫存特徵值中，已出現在其他 IP-MAC 配對中的個數，出現越多重覆的特徵值，此 IP-MAC 配對被冒用的機率越高。
- **計數欄**：特徵值發生異常的次數，次數越多，就越有可能是 IP-MAC 配對遭到了冒用。

欄位如表 3。計數欄的數值會隨著系統運作隨時更新，當有特徵值發生改變後，計數欄的數值就會增加。當計數

欄的數值超過門檻，系統就會開始運算差異欄與重覆欄的數值，當這三個欄位的數值都不為零，甚至是數值很大時，此時管理者就能判斷所監測的 IP-MAC 配對發生了異常。門檻值可隨著觀察的特徵數量與監測環境的特性而自訂。為了幫助管理者能了解區域內發生異常的情形，系統也會將發生特徵值變化的 IP、特徵值內容、發生時間紀錄到另一個資料表，名為異常資料表，如表 4。讓管理者能夠與特徵值紀錄系統進行比對，確認異常的情形為何。

表 4.　異常資料表欄位格式

IP	Data	Time

- **IP:**發生特徵值變化的 IP 位址。
- **Data:**特徵值變化的內容。
- **Time:**詳細的發生時間，格式為月、日、時、分，讓管理者能更詳細的掌握異常發生時間。

IV. 實驗結果

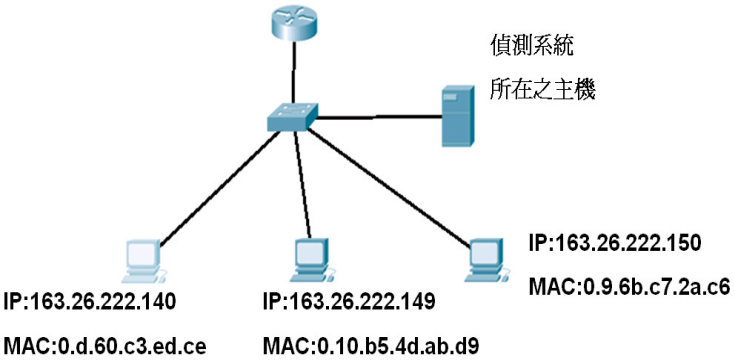

圖 5.　系統測試環境

A.　實驗環境

IP	163.26.222.140	163.26.222.149	163.26.222.150
MAC	0.d.60.c3.ed.ce	0.10.b5.4d.ab.d9	0.9.6b.c7.2a.c6
User-agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB5; KKman3.0; .NET CLR 2.0.50727; InfoPath.1)	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB5)	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6)
出現時間	09:07:09:18	09:07:09:15	09:07:09:15
防毒軟體	kis:rnB-vBumB0vx6-Bv1EzBANNy4wLjEuMzM5	avira:5a566af61f8a442d2710 3a3327d84dfc73cc1e60	Mac:05FE7EF1-F9A6-4553-A54C-7B023325BAB3
出現時間	09:07:09:18	09:07:09:18	09:07:09:17
即時通訊	rokswos@hotmail.com		dpig2001@hotmail.com
出現時間	09:07:09:15	n	09:07:09:15
電腦名稱	T123-532C10DCDA	USER-TEST331	WEI-CECC75A7E7F
出現時間	09:07:09:18	09:07:09:18	09:07:09:18
差異欄	0	0	0
重覆欄	0	0	0
計數欄	0	0	0

圖 6.　系統運作情形

系統的測試環境如圖 5，一共有三個受監測的 IP-MAC 配對，在中央的 Switch 上設定 Port mirror 將所有封包傳送至偵側系統進行紀錄，如沒有 Switch 設備，也可使用 Hub 達到同樣的功能。在下文中將以 IP:後三碼來代表受監測的對像。當系統正常的運作一段時間後，會將所擷取到的特徵值存入資料庫中，成為各 IP-MAC 配對的現有特徵，如圖 6。由於還未有異常情形發生，暫存特徵值皆為空，所以圖中暫不顯示。

B.　模擬冒用情形

我們預設 IP:140 的使用者固定於每天下午七點關機，下班離開。IP:150 的使用者，藉由某些方法如 SMB 封包，取得了 IP:140 的 MAC 位址，並在真正的使用者離開後開始冒用其 IP-MAC 位址。系統會就偵測到如圖 7 的異常情形。在本實驗中，將計數欄的門檻值設為 3，系統偵測到有 3 個特徵值發生了變化。便開始計算差異欄與重覆欄的數值。從圖 7 可以發現，目前 IP:140 這台主機造訪了五個從未去過的網站，而有三個特徵值，同時出現在其他的 IP-MAC 配對之中。參照異常資料表如圖 8,發現變化都是發生在 21 時之後，再利用 SQL 指令查詢，就能發現這些特徵值稍早皆出現在 IP:150 的特徵值中，此時就能明顯的發現是 IP-MAC 配對的冒用。

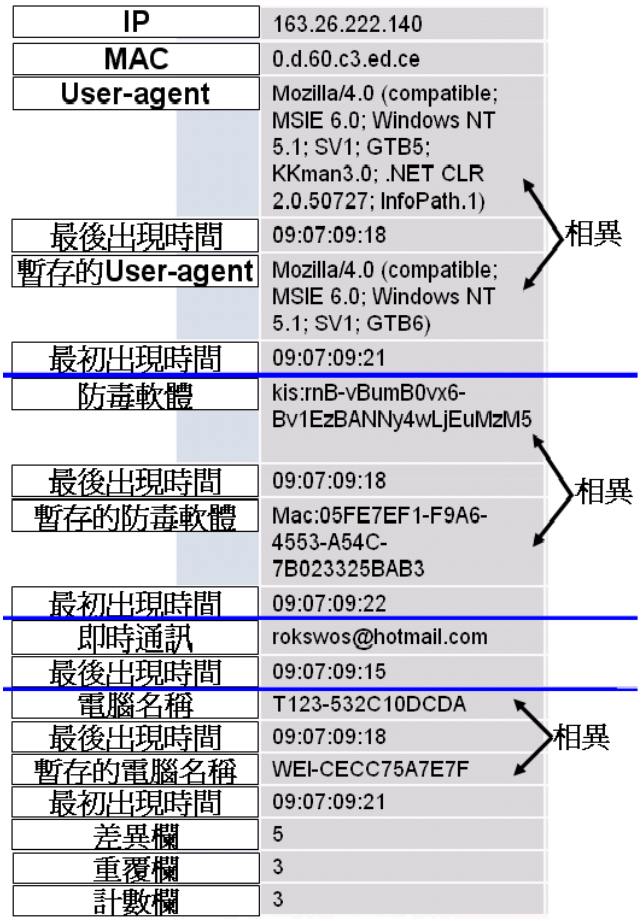

圖 7.　系統偵測到數個特徵值發生了變化

ip	data	time
163.26.222.140	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6)	07:09:21:29
163.26.222.140	WEI-CECC75A7E7F	07:09:21:37
163.26.222.140	Mac:05FE7EF1-F9A6-4553-A54C-7B023325BAB3	07:09:22:15

IP	163.26.222.150
MAC	0.9.6b.c7.2a.c6
User-agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6)
最後出現時間	09:07:09:15
防毒軟體	Mac:05FE7EF1-F9A6-4553-A54C-7B023325BAB3
最後出現時間	09:07:09:17
即時通訊	dpig2001@hotmail.com
最後出現時間	09:07:09:15
電腦名稱	WEI-CECC75A7E7F
最後出現時間	09:07:09:18
差異欄	0
重覆欄	0
計數欄	0

圖 8. 發現冒用的情形

C. *正常更新情形*

當 IP:149 的使用者將主機上的瀏覽器升級之後，這是正常的更新，但系統仍然會偵測到，計數欄也因此變為 1，如圖 9 代表有一個特徵值發生了變化，但計數欄為 1 並沒有大於設定的門檻，所以並不會觸發差異欄、重覆欄的運算。我們實驗預設安全時間為 24 小時，時間的計算由系統自動進行，每當有新的特徵值封包進入，就會與資料庫內暫存最初時間欄位進行比對，看是否有超過 24 小時。暫存特徵值在這 24 小時內不斷的出現，由於新進入的特徵值與暫存特徵值欄位值相符，所以計數欄的數值並不會增加，當特徵值出現超過 24 小時後，而原來的現有特徵值在此 24 小時之內都沒有出現，系統會判斷為正常更新，就會更新現有特徵值，清空暫存特徵值，計數欄歸零，如圖 10。

IP	163.26.222.149
MAC	0.10.b5.4d.ab.d9
User-agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB5)
最後出現時間	09:07:09:15
暫存的User-agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6)
最初出現時間	09:07:10:09
防毒軟體	avira:5a566af61f8a442d27103a3327d84dfc73cc1e60
最後出現時間	09:07:09:18
電腦名稱	USER-TEST331
最後出現時間	09:07:10:09
差異欄	0
重覆欄	0
計數欄	1

相異

圖 9. 更新後偵測到發生變化

IP	163.26.222.149
MAC	0.10.b5.4d.ab.d9
User-agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6)
最後出現時間	09:07:11:09
暫存的User-agent	
最初出現時間	n
防毒軟體	avira:5a566af61f8a442d27103a3327d84dfc73cc1e60
最後出現時間	09:07:10:18
電腦名稱	USER-TEST331
最後出現時間	09:07:11:09
差異欄	0
重覆欄	0
計數欄	0

圖 10. 系統判斷為正常更新

V. 結論與未來發展

本研究所實作的監測系統，的確能夠察覺出所監測的區域裡，所發生的 IP-MAC 配對冒用情形。目前系統只採用了 4 個特徵值來進行紀錄與比對，分別為瀏覽器之 User-agent、防毒軟體識別碼、即時通訊軟體帳號、電腦名稱，主要是因為這 4 個特徵值皆能在受監測者無從發覺的情況下，就能透過網路上所傳送封包取得。在日後也能依據監測環境的不同，將其它可利用的特徵值加入系統之中，如各大專院校的校務系統常使用的學號、教職員帳號等，也能與校園授權軟體廠商進行配合，取得其用來驗證使用者的識別碼，並預設授權軟體的更新時間，讓系統能在固定的時間內能不斷的對特徵值進行比對，提高系統辨識的準確度，縮短發現冒用的時間。

參考文獻

[1] 姜文忠，廖述益，施銘亮，“網頁式校園宿舍網路管理資訊系統規劃與建置”，TANET 2007 台灣網際網路研討會論文集(一)，pp. 125–129，2007 年 10 月

[2] 楊文龍，陳彥錚，“基於 SNMP 之 ARP 攻擊偵測研究”，TANET 2008 台灣網際網路研討會論文集(一)，pp. 317–322，2008 年 10 月

[3] 郭蕭禎，謝進利，許忠強，“以 SNMP 偵測阻斷區域網路 ARP 欺騙行為”，TANET 2008 台灣網際網路研討會論文集(一)，pp. 272–277，2008 年 10 月

[4] 任善隆，許俊萍，孫際宇，“宿舍網路維運與 IP 流量限制方案”，TANET 2005 台灣網際網路研討會，2005 年 10 月

[5] http://msdn.microsoft.com/zh-tw/library/cc817582.aspx

[6] http://zh.wikipedia.org/w/index.php?title=SMB&variant=zh-tw

[7] http://www.google.com.tw