ARP Spoofing 偵測及防護機制-以 Arcai Netcut 軟體為例

王永鐘　王宜秀
國立臺北科技大學　計算機與網路中心
國立臺北科技大學　電機工程系
ycwang@ntut.edu.tw　t100318117@ntut.edu.tw

摘要

Address Resolution Protocol (ARP)是電腦主機用以轉換網路位址(IP Address)至實體位址(MAC address)的網路協定，ARP spoofing 則藉由 ARP 沒有防護機制的弱點而產生的網路攻擊手法，例如在區域網路發動 Denial of Service (DoS) 及 Man In The Middle (MITM)攻擊，ARP 的缺點所造成的網路攻擊不但可能會癱瘓網路運作，甚至個人資料也會透過 ARP spoofing 而被竊取。本論文以 ARP spoofing 軟體為研究對象，分析 Arcai Netcut 軟體運作原理及其造成的網路影響，並建立一套分散式架構、快速、有效、低成本的自動偵測及防護 Arcai Netcut 解決方案，本研究整合 Command-Line Interface (CLI) 功能及各式 Linux scripts，本系統已成功運作於學生宿舍網路及校園網路並有效偵測及防護 Arcai Netcut。

關鍵詞：ARP spoofing、DoS、MITM、Arcai Netcut

Abstract

Address Resolution Protocol (ARP) is one of heavily used protocols by computers for mapping network address (IP address) to physical address (MAC address). ARP spoofing is a deception within the LAN caused by ARP flaws, which is used to launch Denial of Service (DoS) and Man In The Middle (MITM) by attackers. ARP flaws could cause the network paralyzed and even worse personal information stolen through ARP spoofing attack. In this paper, we analyzed the process and the effect of the common ARP spoofing software called Arcai Netcut. A distributed, swiftly, effective, and low cost solution, which could automatically detect and defense the Arcai Netcut is implemented on Linux Mini PC. We combined the functions of Command-Line Interface (CLI) and some different Linux scripts to develop the software, which succeed in detecting and defensing the Arcai Netcut in the student dormitory network and campus network.

Keywords: ARP Spoofing、DoS、MITM、Arcai Netcut

1. 前言

隨著網路應用服務愈來愈多元，其中影音訊務頻寬需求愈來愈大，當網路壅塞時，不少網路使用者便嘗試上網尋求可提高網路連線速度的方法，或者使用可影響其他網路使用者的軟體；若是採用調整區域網路架構、從集線器(hub)改用交換器(switch)或者調整作業系統設定值等方式都是正確且不影響他人的作法，但是對電腦網路運作知識不了解的人，可能會誤用含有網路惡意行為的軟體，例如 Arcai Netcut 軟體便是其中之一[1]，該軟體運作機制即是 ARP spoofing[2]，程式啟動後對同網段中其他電腦發動 Denial of Service (DoS)[3]攻擊，使其他電腦無法取得正確 gateway MAC 位址而無法上網，但是 Arcai Netcut 軟體使用者卻可以正常上網，原作者還提供 Netcut Defense 軟體來防禦 Arcai Netcut 攻擊，如此矛盾的兩款軟體，造成骨幹網路充斥大量 ARP 封包，使骨幹網路設備 CPU 使用率快速上升，在骨幹網路設備相當忙碌的狀態下產生 packets drop 及網路斷斷續續的現象。

Arcai Netcut 使用者大多位於共享網路頻寬的學生宿舍網路及校外租屋環境，有時為了保障自身使用網路頻寬的權益，有時為了阻止其他佔用網路頻寬進行大量下載的使用者，不管是以何種原因安裝 Arcai Netcut 軟體，一旦在區域網路內運行 Arcai Netcut，立即會使區域網路變得壅塞及忙碌。

目前已有不少針對 ARP spoofing 弱點而提出的解決方案[4]，大致上分為三類，一、加密式 IP/MAC[5]、二、Host-based[6]、三、Server-based[7]；不論是以非對稱式加密將 ARP 封包進行交換，或是在個人電腦安裝 Agent 程式，甚至以集中式控管所有 ARP 封包的方式，大多需要在 PC 端安裝程式或進行電腦參數的調整；本研究以不影響住宿學生的電腦環境，卻又能在短時間發現 Arcai Netcut 的運作，並且有效阻止 Arcai Netcut 所造成的網路不良影響為目標，著手進行各種可能的解決方案。

本文之架構如下：第二章簡介 Address Resolution Protocol(ARP)的運作原理；第三章簡介數個可以有效防禦 ARP spoofing 的系統，以及這些系統的優缺點；第四章為系統設計，詳細介紹本研究的作法及運作流程，並且展示實際應用於學生宿舍網路及校園網路的成果。

2. 地址解析協定簡介

地址解析協定 Address Resolution Protocol(ARP)網路協定是用於將 32 位元的 IP 位址與 48 位元的

MAC 位址之間進行轉譯[8]，是 IPv4 中網路層必要的協定，ARP 運作流程如下：首先，若電腦 A 想與電腦 B 進行通訊，電腦 A 會先在自身的 ARP table 中查詢電腦 B 的 IP 位址及 MAC 位址對應紀錄，若該對應紀錄存在，則電腦 A 將電腦 B 的 MAC 位址填入 Data Link 層的封包表頭，再將封包發送出去，若該對應不存在，則電腦 A 會以 broadcast 方式，對同網段所有電腦發送 ARP 請求封包，電腦 B 收到該 ARP 請求封包後，將自身的 MAC 位址填入 Data link 層封包表頭，再用 unicast 方式將封包回送給電腦 A，電腦 A 將封包中電腦 B 的 IP 位址及 MAC 位址對應更新 ARP table，由於 ARP 請求封包的發送端只管接收回應的封包訊息，無法對封包內容真偽進行分辨，所以利用此 ARP 網路協定的弱點就可以在區域網路中發動 Denial of Service(DoS)及 Man In The Middle(MITM)[9]等網路攻擊。

3. 防範 ARP 網路攻擊相關研究

列舉數個已發表且可以有效防護 ARP spoofing 的解決方案內容及其優缺點：

3.1 基於 SNMP 及 WinPcap 之 ARP Spoofing 即時偵測及恢復

此研究整合 SNMP 及 WinPcap 功能達到 ARP spoofing 即時偵測及恢復的效果[10]，該研究於 Windows 平台安裝 WinPcap 程式，由於 WinPcap 程式具有讀取封包及解析封包的能力，可藉由撰寫 WinPcap filter 程式，不斷監聽區域網路中所有網路封包，然後判斷區域網路中是否有 ARP spoofing 事件，即時發現 ARP spoofing 來源的 MAC 位址，將判斷結果交給 Linux 平台，以 SNMP 指令查找 ARP 攻擊者所在 switch port，再以 SNMP 指令關閉該 switch port，可立即阻絕 ARP spoofing 運作；此研究需協同二種作業系統平台，且 mirror 大量區域網路資料流，此作法恐對 Windows 平台造成效能衝擊，而在 switch 開放 SNMP 寫入的作法方面，若 switch IP 及 SNMP community 名稱被發現，則 switch 可能被有心人士進行操作，恐造成資安事件。

3.2 動態 ARP spoof 問題防護系統

該研究於 DHCP 網路環境中架設 Linux 平台伺服器當作 gateway，將所有 DHCP 封包中 IP/MAC 對應紀錄保存，並於同網段中各個電腦安裝 Agent 程式，在電腦開機時，由 Agent 程式向 gateway 取得所有電腦的 IP/MAC 對應紀錄，並寫入自身 static ARP table 中，可防止 ARP spoofing 攻擊[11]，一旦 Agent 程式收到 ARP 請求與回應封包時，Agent 程式將與自身的 static ARP table 比對，比對結果有差異時，就是發生 ARP 攻擊事件，此時再通過數位簽章的方式將訊息傳達給同網段的監控伺服器，該伺服器以簡訊、MSN 訊息、Email 及 log 四種方式告警網路管理員，以達到自動化監控及防護機制；此解決方案適用於小型 DHCP 的網路環境，且需要於所有電腦主機安裝 Agent 程式，用以向 gateway 取得同網段中所有電腦的 IP/MAC 對應紀錄，然後寫入自身的 static ARP table 中，安裝 Agent 程式的作法對於校園網路或企業網路為數眾多且作業系統不一的電腦主機來說，將是一種管理負擔。

3.3 輕量化 IP-ARP Spoofing 偵測及預防系統

此解決方案以分散式架構運作，以達成輕量化 IP-ARP spoofing 偵測及預防目的[12]，首先，在各個閘道器架設流量監控伺服器，各網段的電腦設備均需安裝 Agent 程式，在電腦開機後，Agent 程式發送本機 IP/MAC 對應紀錄給流量監控伺服器，同時 Agent 程式在背景不斷將本機發送的 ARP 請求封包、ARP 回應封包、ARP 封包數量及發送時間間隔等資訊給流量監控主機，各流量監控主機擁有各網段所有電腦正確的 IP/MAC 對應紀錄，一旦與 Agent 程式比對送來的 ARP 訊息有差異時，即可確定發生 ARP 攻擊事件，流量監控主機即時將所有的正確 IP/MAC 對應資料傳送給被攻擊電腦，以確保被攻擊的電腦可以重新取得所有正確的 IP/MAC 對應紀錄及恢復正常網路運作，在 ARP 攻擊事件發生時，同時以防火牆阻擋異常流量，如此可使被攻擊電腦恢復正常網路連線及防止 ARP 攻擊流量擴散；此解決方案有分散式管理及快速有效的優點，但是無法找到 ARP 攻擊者的所在網路位置，且需要在不同作業系統平台安裝 Agent 程式，若電腦數量眾多，也有管理及安裝 Agent 程式的困難。

4. ARP Spoofing 偵防系統設計

本研究整合網路設備 Command-Line Interface (CLI) 功能[13]，定時運作 Linux minicom script 連接網路設備 console 介面[14]，並下達 debug arp 及 no debug arp 指令，建置 Linux syslog server 蒐集網路設備 ARP log[15]，使用 Linux shell script 解析及排序 ARP log 內容[16]，即可找出 Arcai Netcut 使用者的 IP 及 MAC 位址，再透過 Linux shell script 對學生宿舍所有 Layer-2 switch 下達 SNMP 指令，查詢 Arcai Netcut 使用者所在 switch port No. [17,18]，最後透過 Linux telnet script 關閉 Arcai Netcut 使用者所在網路節點，以達到自動偵測及防護 Arcai Netcut 的目標[19]。

本研究的 ARP spoofing 攻擊偵測及防禦系統實作目標以分散式架構、快速、有效、低成本等前提下進行，可發動 ARP 攻擊的常見軟體有：用於中間人攻擊的 Cain & Abel[20]，用於修改封包內容然

後使用的 Packet Builder[21]，以及用於發送大量 ARP 阻斷封包造成 Denial of Service (DoS)攻擊的 Arcai Netcut 等，其中以 Arcai Netcut 最常被學生使用於宿舍網路，使自己可以佔用網路頻寬，同時造成其他同學無法上網及骨幹網路設備 CPU 使用率瞬間提高等現象，為阻絕 Arcai Netcut 所造成的影響，本研究針對 Arcai Netcut 進行自動偵測及防禦系統實作，詳細實作內容於下列各節說明。

4.1 Arcai Netcut 網路剪刀手運作原理

網路攻擊者常用 Arcai Netcut 發送大量 ARP 回應封包至區域網路中所有電腦，這些 ARP 回應封包都是包含偽造的 gateway MAC 位址，由於 ARP 協定的弱點，被攻擊的電腦收到 ARP 回應封包時，無法驗證真偽，所以即使收到偽造的 gateway MAC 位址，也會取用並更新自身的 ARP table，如此一來，在收到大量惡意的 ARP 回應封包後，被攻擊者將無法與正確 gateway MAC 位址聯繫而無法上網。

圖 1 為 Arcai Netcut 開始執行運作時畫面，該軟體會先掃描同網段所有 IP，得知各電腦是否於網路上運作，並向同網段所有 IP 發送 ARP 請求封包，以 broadcast 方式發送每秒鐘約 60 個 ARP 請求封包，以取得同網段所有 IP 的 MAC 位址，如下圖 2 所示，再以 Arcai Netcut 選擇發動 Denial of Service(DoS)攻擊的對方 IP 後，隨即針對該 IP 發送大量內含偽造 gateway MAC 的 ARP 回應封包，由於被攻擊者無法取得正確的 gateway MAC 位址而無法上網。

圖 1 Arcai Netcut 程式啟動畫面

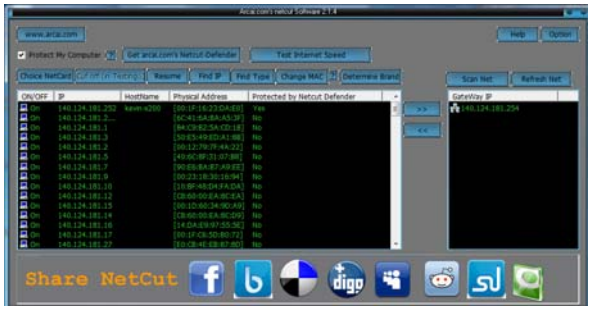

圖 2 Arcai Netcut 顯示同網段各電腦 IP/MAC

4.2 CISCO Layer-3 switch 功能

本校校園網路以常見的三層式網路架構建置而成，其中核心層為 CISCO 6509，匯聚層為 CISCO 3750，而存取層為 CISCO 2960；當有電腦開始運作 Arcai Netcut 時，不斷以 broadcast 的方式發送每秒鐘約 60 個 ARP 請求封包，向同網段所有 IP 送出 ARP 請求，此時由於 CISCO 3750 收到大量 ARP 廣播封包而使 ARP Input 程序 CPU 使用率立即提高，下圖 3 為執行 Arcai Netcut 後，CISCO 3750 CPU 即時使用率，而下圖 4 為一日之中各時段使用 Arcai Netcut 對 CISCO 3750 CPU 使用率的統計圖。

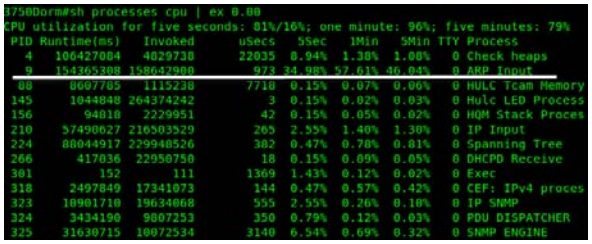

圖 3 CISCO3750 CPU 即時使用率

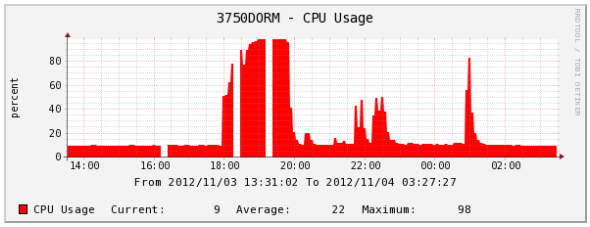

圖 4 CISCO 3750 CPU 使用率統計圖

在 CISCO 3750 的 CLI 指令裡，可用下表 1 所示指令查看即時 ARP 請求及回應封包細節，ARP 相關訊息都會被儲存於 CISCO 3750 log 之中，如下表 2 所示，透過 syslog server 自動收集 CISCO 3750 log，並以 Linux shell script 自動解析並排序 log 內容，即可找出發送大量 ARP 請求封包的來源 IP/MAC 位址。

表 1 CISCO ARP 封包查看指令

指令	用途
debug arp	開啟 ARP debug mode
no debug arp	關閉 ARP debug mode

表 2 CISCO ARP debug log 內容

log 類型	log 內容
ARP 請求封包	IP ARP : rcvd rep src 140.124.135.122 b888.e3a0.d88f, dst 140.124.135.254 Vlan134
ARP 回應封包	IP ARP : sent rep src 140.124.135.254 0026.0ba1.fec2, dst 140.124.135.122 b888.e3a0.d88f Vlan134

4.3 Arcai Netcut 偵測及防護機制運作流程

由於 CISCO 3750 提供 debug arp 指令功能，所以無需使用 Windows 平台的 WinPcap 軟體對區域網路所有流量進行即時分析，就可以透過收集、解析及排序 ARP log 找到大量發送 ARP 請求封包的來源 IP/MAC 位址；本系統使用一台 Mini PC，安裝 Linux CentOS 6 作業系統，使其與 CISCO 3750 的 console 及 LAN 相接，如下圖 5 所示。

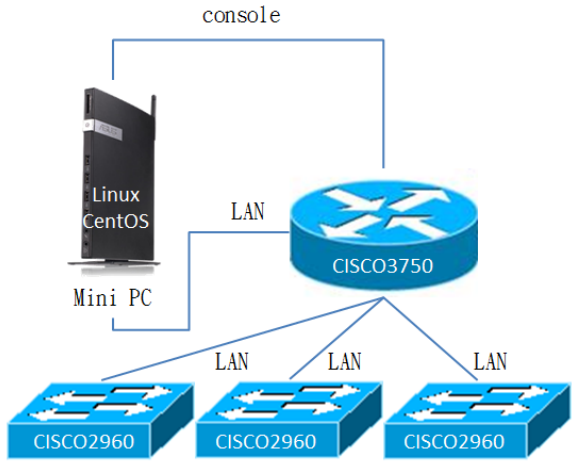

圖 5 Mini PC 與 CISCO 3750 架構圖

Mini PC 每 10 分鐘執行 Linux minicom script 連接 CISCO 3750 console 介面，使 CISCO 3750 執行 10 秒鐘 debug arp 指令，將 ARP log 以 syslog 的方式在 LAN 環境下傳送給 Mini PC，再使用 Linux shell script 解析及排序 log 內容，即可自動化得到大量發送 ARP 請求封包的來源 IP/MAC 位址，如圖 6 所示。

```
20130110-13:32:18
  count request-IP      request-MAC
    838 140.124.131.17:0024.1da6.d3e8
     11 140.124.141.155:50e5.493e.f1db
      9 140.124.147.251:001d.6054.469b
      7 140.124.135.43:bcf6.85a8.2f96
      6 140.124.135.31:5404.a61f.5990
      5 140.124.147.107:bcae.c51d.0723
      5 140.124.135.164:3085.a918.b7cd
      4 140.124.144.194:000e.c6f0.2090
      4 140.124.141.165:c860.0021.f3dc
      4 140.124.141.154:dc0e.a11f.f630
```

圖 6 10 秒鐘內 ARP 請求封包統計 TOP 10

經過多次實驗後得到的統計結果，我們發現在 10 秒鐘內發送超過 500 筆 ARP 請求封包者，即是使用 Arcai Netcut 使用者，我們可以從 ARP log TOP 10 統計結果得知 Arcai Netcut 使用者的 IP/MAC 位址，接著 Mini PC 傳送 SNMP 指令給 CISCO 3750 底下所有 CISCO 2960 的 FDB (forwarding database) table，查找 Arcai Netcut 使用者 MAC 位址所在 switch port No.，相關的 MIB(Management Information Base)值分別為：dot1dTpFdbAddress OID, 1.3.6.1.2.1.17.4.3.1.1 及 dot1dTpFdbPort OID, 1.3.6.1.2.1.17.4.3.1.2，Mini PC 得到 Arcai Netcut 使用者所在 CISCO 2960 switch port No.後，再執行 Linux telnet script，將該 switch port 關閉，即可阻絕 Arcai Netcut 使用者，完整自動化偵測及防護流程如下圖 7 所示。

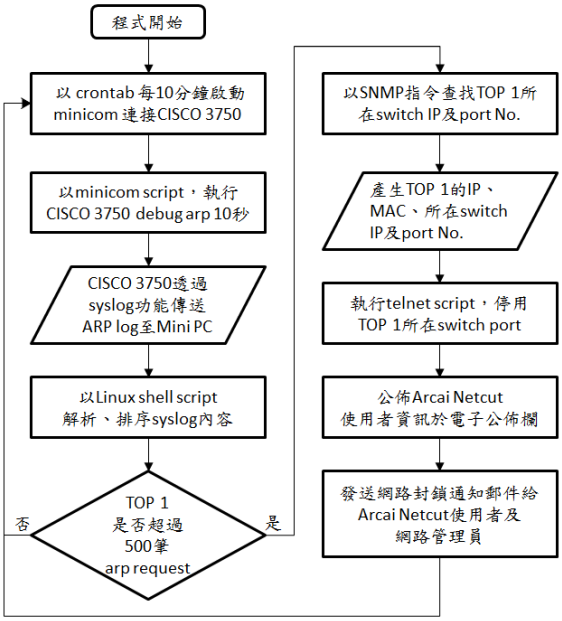

圖 7 自動化偵測及防護 Arcai Netcut 流程

本系統自動封鎖 Arcai Netcut 使用者網路後，立即透過電子郵件方式通知使用者及網路管理員，並且公佈部分使用者個人訊息於液晶電視公佈欄，如下圖 8 所示，待使用者移除 Arcai Netcut 並回覆電子郵件後，再由網路管理員解除網路封鎖限制。

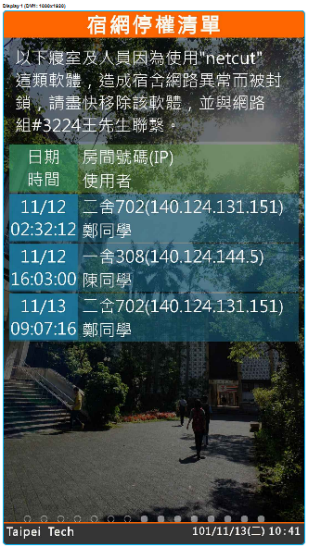

圖 8 公告 Arcai Netcut 使用者資訊

4.4 系統運作成果

本系統於學生宿舍自動偵測及防範 Arcai Netcut 使用者的成效顯著，因此複製相同的網路架構至全校校園網路，如下圖 9 校園網路架構圖，經由統計全校每月 Arcai Netcut 事件，得到如表 3 統計結果，本系統於全校運行後，雖然仍有少數使用 Arcai Netcut 事件，但已無法對校園網路造成影響，以及不再發生因 Arcai Netcut 而使學生無法上網的情形，以 8 個月的系統運作成果顯示，可驗證本系統具有效偵測及防範 Arcai Netcut 於校園網路中運作的能力。

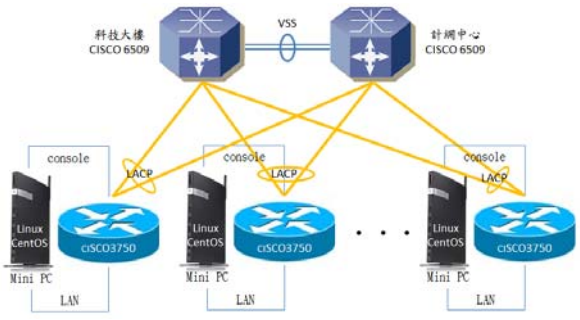

圖 9 擴大本系統至全校網路架構

表 3 全校 Arcai Netcut 事件統計表

民國年/月	101/10	101/11	101/12	102/1	102/2	102/3	102/4	102/5	102/6	102/7
全校Arcai Netcut 事件總數	1	7	4	7	5	5	4	6	0	0

5. 結論

本研究整合網路設備提供的 CLI 指令，debug arp 功能，搭配一台 Linux CentOS Mini PC，透過撰寫各式 scripts，以達到自動偵測及防護 Arcai Netcut ARP spoofing 網路攻擊，本研究初期於學生宿舍網路運作，因為成效良好，接著擴及全校校園網路，成功達到分散式架構、快速、有效、低成本的目標；由於 ARP 網路攻擊日新月異，本研究未來可朝以下幾個方向發展：

(1)具備對各廠牌 Layer-3 switch 進行 ARP spoofing 網路攻擊偵測及防護的能力。

(2)縮短偵測時間，達到即時偵測及防禦大量使用者同時進行 ARP 網路攻擊的能力。

參考文獻

[1] “Arcai Netcut,” http://arcai.com/

[2] http://en.wikipedia.org/wiki/ARP_spoofing, accessed Sep. 2012.

[3] Kumar, S., “Impact of distributed denial of service (DDoS) attack due to ARP storm,” Lect. Notes Comput. Sci., 2005, 3421, pp. 997–1002.

[4] M. Oh, Y.-G. Kim, S. Hong, S. Cha, “ASA: agent-based secure ARP cache management,” IET Communacation., vol. 6, no. 7, 2012, pp. 685-693.

[5] Bruschi, D., Ornaghi, A., Rosti, E., “S-ARP: a secure address resolution protocol,” Proc. 19th Annual Computer Security Applications Conf. (ACSAC2003), Las Vegas, NV, USA, December 2003, pp. 66–74.

[6] Xing, W., Zhao, Y., Li, T., “Research on the defense against ARP spoofing attacks based on WinPcaP,” Proc. Second Int. Workshop on Education Technology and Computer Science (ETCS2010), Wohan, China, March 2010, pp. 762–765.

[7] Gouda, M.G., Huang,C.T., “A secure address resolution protocol,” Comput. Netw.: Int. J. Comput. Telecommun. Netw., vol. 41, no. 1, 2003, pp. 57–71.

[8] RFC-826, “An ethernet address resolution protocol,” 1982.

[9] “Man In The Middle,” http://en.wikipedia.org/wiki/Man-in-the-middle_attack,

[10] L. Wang, Y.-S. Li, L.-wei Hu, “Real-time detection and recovery of ARP Spoofing based on SNMP and WinPcap,” 2012 IEEE Internation Conference on Cyber Technology in Automation, Control, and Intelligent System(CYBER), 2012, pp.1-4.

[11] S. Puangpronpitag, N. Masusai, “An Efficient and Feasible Solution to ARP Spoof Problem,” IEEE, 2009, pp.2-3.

[12] S. G. Bhirud, V. Katkar, “Light Weight Approach for IP-ARP Spoofing Detection and Prevention,” 2011, pp.3-4.

[13] Cisco Systems, “Configuring Dynamic ARP Inspection,” Catalyst 6500 Series Switch Cisco IOS software Configuration Guide, Release 12.2SX, chapter 56.

[14] “Linux/UNIX minicom Serial Communication,” http://www.cyberciti.biz/tips/connect-soekris-single-board-computer-using-minicom.html

[15] “Configuring a syslog server on RHEL/CentOS 6,” http://people.opencomputingsolutions.com/?p=53

[16] “Linux Shell Scripting Tutorial v1.05r3 A Beginner’s handbook,” http://freeos.com/guides/lsst/

[17] “Cisco SNMP Object Navigator,” http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

[18] “SNMP Command Examples,” http://docs.oracle.com/cd/E19201-01/820-6413-13/SNMP_commands_reference_appendix.html

[19] “Telnet Scripting with Bash-Linux,” http://amilasurendra.info/telnet-scripting-with-bash-linux/

[20] “Packet Builder, ” http://www.colasoft.com/packet_builder/

[21] “Cain&Abel, ” http://www.colasoft.com/packet_builder/