防範位置解析協定攻擊癱瘓區域網路 —

以網路剪刀手與批次檔為例

Take Precautions about Address Resolution Protocol Spoofing

paralyze Local Network – Using NetCut and Batch File

張凱慕　陳雅萍　姜自強

興國管理學院資訊管理學系

b911010065@std.hku.edu.tw

摘要

在這個廣大無疆的網路世界裡，常常預埋了許許多多的危機，在區域網路（Local Area Network）中更是如此，位置解析協定（Address Resolution Protocol）在區域網路中，扮演著不容忽視的角色，其主要被設計用於以 OSI model 第三層位址（IP address）求得第二層位址（MAC 位址），我們針對位置解析協定（Address Resolution Protocol），使用網路剪刀手(NetCut) 做了一連串的實驗，其目的在強調位置解析協定（Address Resolution Protocol）的危險性，我們透過觀察實驗的結果，發現市面上的防火牆，幾乎不具有即時防止「欺騙位置解析協定攻擊（ARP Spoofing Attack）」的功能，綜觀本次實驗我們發現，「欺騙位置解析協定攻擊（ARP Spoofing Attack）」，對區域造成極大的威脅，於是我們提出了一些方法，在區域網路（Local area network）建立的時候，便將批次檔（Batch file）加入開機時序，同時並搭配網際網路控制訊息協定（Internet Control Message Protocol）這一個通訊協定，此時電腦會不定時的更新，並同時固定部分的區域網路位置(Local Area Network IP address)，並將其寫入 ARP Table 若依照此方法便可以防範「欺騙位置解析協定攻擊（ARP Spoofing Attack）」癱瘓區域網路這一個棘手的問題。

關鍵字：位置解析協定(Address Resolution Protocol , ARP）、欺騙位置解析協定攻擊（ARP Spoofing Attack）、批次檔（Batch file）。

1.前言

網際網路的日益發展，在這一個虛擬的國度裡，有人矢志於建設，也有人立志於破壞，而在IPV4的世界中，因為網際網路協定位置（IP Address)的數目不夠，所以「位置解析協定(Address Resolution Protocol）」是一個不可缺少的通訊協定，此外建立區域網路（Local area network），也是一種普遍解決網際網路協定位置（IP Address）數目不足的方式之一，但是在區域網路（Local area network）中，大多數的人都使用相同的預設閘道(gateway)、子網路遮罩(Subnet Mask)，而這些相同的設定往往卻造成了許許多多不可避免的危險，像是木馬程式、系統安全等問題，雖然大部分的後門程式可以透過使用防毒軟體來避免，系統安全可以藉由定時更新來降低危險性，在必要時還可以加裝防火牆來阻擋，但是「欺騙位置解析協定攻擊（ARP Spoofing Attack）」卻是不易避免的，於是我們先設計一個小實驗，藉由在實驗的過程中，找到封包資料，並做分析。

在實驗的過程中，我們使用「網路剪刀手（Netcut）」和「Ethereal」這兩套軟體來進行我們的實作，首先在網路剪刀手（Netcut）的部分，它在實驗裡扮演著一個非常重要的角色，它負責不斷

的發送錯誤的「位置解析協定(Address Resolution Protocol)」封包，來塞滿 ARP Table，目的用以阻斷想要攻擊的主機連線，而Ethereal在這裡扮演著一個紀錄者的角色，在整個攻擊的過程中，它負責將一切封包記錄下來，方便我們分析整個攻擊的狀況。

2.文獻探討

2.1 通訊協定簡介

國際標準組織（International Organization for Standardization，ISO）和國際電訊聯盟(International Telecommunication Union，ITU）的電訊標準化部門（Telecommunication Standardization Sector）為解決網路間不相容與彼此、無法溝通的問題，研究如 DECNET、SNA 之類的網路架構後，於 1984 年發表 OSI （Open System Interconnection）網路七層參考模型，其目地是提供網路的標準模型以促使各個不同公司之間的設備能夠互相溝通，並為全世界許多生產各種不同網路產品的公司提供設計及開發的參考。而目前網際網路上通用的 TCP/IP 協定，則是 1970 年代美國國防部（Department of Defense，DoD）基於戰爭需求，需要一種能夠在任何情況下，且不論網路中任何特定節點的狀況如何，都能讓資訊隨時由任何一點傳到另一點，所發展出的一套網路協定，除了上述兩種，另外還有一種是 Microsoft Network，其三種的相對關係如下圖。

圖 2.1　網路協定比較圖

2.2 位置解析協定

位置解析協定(Address Resolution Protocol)，主要被設計用於以 OSI model 第三層位址（IP address）求得第二層位址（MAC 位址），ARP 封包只會在同一個子網路（subnet）內傳送，它很少透過路由器（router）傳送至不同的網路。主機的作業系統會依照封包目地 IP 位址與本機之子網路遮罩（subnet mask）的值進行運算，以判斷封包目地 IP 是否與本機同屬於一個子網路。位置解析協定（Address Resolution Protocol）是一個非常重要且使用頻繁的協定，在任何一個 TCP/IP 的連線被建立之前，都必需經由位置解析協定（Address Resolution Protocol）取得目地主機的實體網路位址（MAC），在區域網路（Local area network）中，這是普遍且不容忽視的協定，也是我們這次主要鎖定的目標。

2.3 欺騙位置解析協定（ARP Spoofing）

欺騙位置解析協定（ARP Spoofing），市面上有很多軟體，它主要是要讓 OSI 的第二層和第三層無法連接，並癱瘓其網路，而在這眾多軟體之中，研究者偏好使用網路剪刀手（NetCut），它的原理是，負責假造 ARP 封包，提供給目標主機假的實體網路位址(MAC)資訊，通訊閘道(Gateway)收到後，於是將錯誤的實體網路位址（MAC）記到 ARP Table 內，伺服端（Client）的返回封包就無法送達，也就無法上網，於是我們使用這一套軟體，進行下列一連串的實驗。

3.研究方法

在區域網路（Local area network）中，我們經由文獻探討發現，位置解析協定（Address Resolution Protocol），本身充滿著許許多多的危險性，於是我們進而去求證，我們使用了網路上著名的駭客軟體－網路剪刀手（Netcut）做出欺騙位置解析協定攻擊 (ARP Spoofing Attack)，然後檢視它

的封包和結果，並證明它是否真的對區域網路（Local area network）造成威脅，於是我們針對這個狀況，希望提出能夠改善現況的方法。

（1）本研究的實驗架構，先分別將兩台主機，命名為目標主機和攻擊主機，此外分別將兩台主機，接至集線器（HUB）上，並分別在兩台電腦裝上，Ethereal 和網路剪刀手（Netcut）並開始作測試，架構如圖 3.1。

圖 3.1　實驗架構圖

（2）架設好硬體環境，於是開始設置網際網路協定位置(IP Address)目標主機為「192.168.1.10」，攻擊主機為「192.168.1.15」，子網路遮罩(Subnet Mask)都為「255.255.255.0」，預設閘道(Gateway)都為「192.168.1.1」，於是我們分別在兩台電腦，鍵入「ipconfig」，結果如圖 3.2.1 當檢視完基本設定無誤後，我們鍵入「ping」結果如圖 3.2.2。

目標主機	攻擊主機
	

圖 3.2.1　檢視網路基本設定

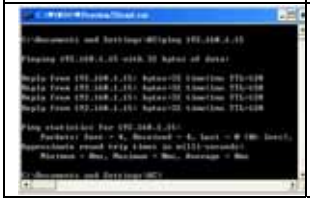
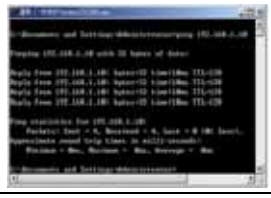
目標主機	攻擊主機
	

圖 3.2.2　判斷區域網路是否建立

（3）於是我們打開，網路剪刀手（Netcut），首先我們選擇我們的網卡「00-0F-EA-44-73-87」，然後在我們打開網路剪刀手（Netcut）的同時，它會自行尋找在這區域網路（Local area network）下有幾台電腦。

圖 3.3　攻擊介面

（4）我們打開 Ethereal，然後一樣，我們選擇網卡，再進而做些小測試，當我們開始擷取封包的時候，我們使用終端機介面，鍵入「ping 192.168.1.15」，用以測試此時的兩台主機是否存活。

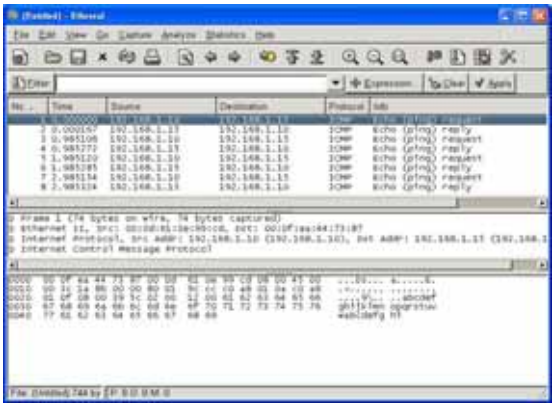


圖 3.4　封包擷取介面

（5）經由上述的測試，我們的兩台主機功能都正常，於是我們開始進行攻擊，首先我們把預設的預設閘道(Gateway)改成攻擊主機的 IP 位置

「192.168.1.1 → 192.168.1.15」。

圖 3.5　攻擊開始

（6）我們擷取封包發現，當 ICMP 協定，沒有反應的時候，也證明我們成功的癱瘓目標主機「192.168.1.10」。

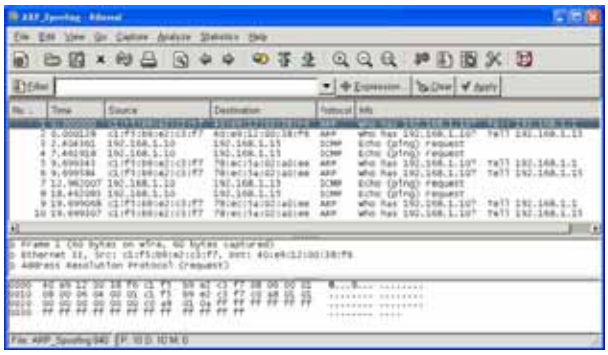


圖 3.6　封包紀錄圖

經過一連串的實驗，我們發現大部分的防火牆都沒有辦法及時的來處裡這個問題，但是欺騙位置解析協定攻擊（ARP Spoofing Attack）的危機卻時時刻刻威脅著我們網路的安全，駭客們可能利用一個大意的使用者，進而癱瘓整個網路，於是我們提出一個能夠將其傷害減到最輕的辦法，因為欺騙位置解析協定攻擊（ARP Spoofing Attack）大多都是以程式，製造 ARP 封包，提供目標電腦的假實體網路位址（MAC）資訊，預設閘道（Gateway）收到後，就將錯誤的實體網路位址（MAC）記錄到 ARP Table，伺服端（Client）的返回封包就無法送達，也就成功的癱瘓區域網路（Local area network）。

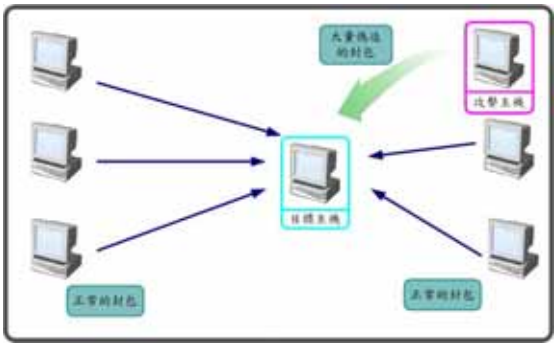


圖 3.7　示意圖

經過我們幾番思量，我們發現要解決這個問題技術面其實並不困難，針對它的原理要克服這一個障礙並不困難，但若是要做到即時防護，這就需要相當的技巧，於是我們查閱了一些相關文獻，發現到其實我們可以把已知的實體網路位置（MAC）、IP 將其固定，但是往往都要等攻擊發生才能去預防，於是我們加入時序的功能，讓電腦分別在開機的時候會固定住一部分的實體網路位置（MAC）、IP 於是我們將部分指令在開機時會自動執行，並製作即時批次檔(Batch file)，並附上時序，雖然這方法不能根治欺騙位置解析協定攻擊（ARP Spoofing Attack），但是卻可以防範於未然，把這個攻擊發生的機率降到最低。

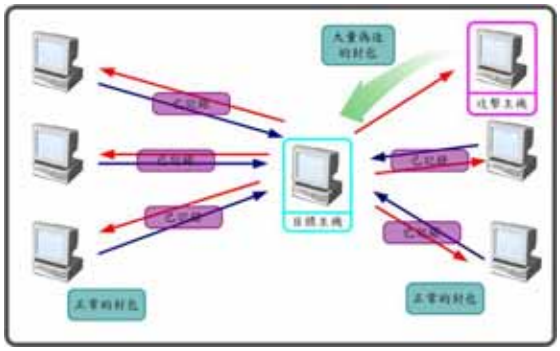


圖 3.8　解決辦法剖析圖

針對即時批次檔(Batch file)的部份，我們在批次檔裡利用 ICMP 協定，用以判斷主機是否存活，如果存活就會更新 ARP Table，把原本浮動的 ARP 固定住，區域網中大部分存在的主機，使用者的 ARP Table 上面都有對應的 MAC，如此這

般，我們在短時間被塞滿的 ARP Table 依然能夠保有他部分的功能，不至於對方一發動欺騙位置解析協定攻擊（ARP Spoofing Attack）的同時，網路立即呈現癱瘓的狀態。

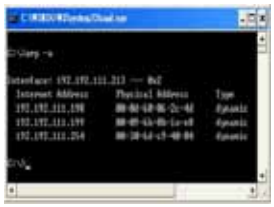
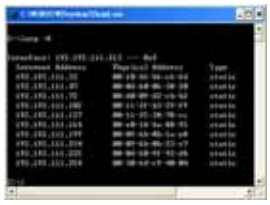
使用批次檔前	使用批次檔後
	

圖 3.9　使用批次檔前後對照

4.結論及未來展望

欺騙位置解析協定攻擊（ARP Spoofing Attack）確實在區域網路（Local area network）中具有極大的威脅，無可否認的目前的技術卻沒有一個完善的機制能夠徹徹底底的解決這個問題，加上一般常用的防火牆並沒有針對欺騙位置解析協定攻擊（ARP Spoofing Attack）做出一些預警的功能，然而我們所提出的方法雖然不能夠徹底的根治這一個問題，但是我們這個方法，可以在受攻擊前做好防範的措施，雖然這一個方法不是非常的高明，技術不是非常的艱深，但是針對欺騙位置解析協定攻擊（ARP Spoofing Attack）卻能夠有效地降低發生率。

我們在尋找解決之路上，面臨了些許的困難，如何紀錄有效的 ARP 封包，如果我們將所有的 ARP 封包都標上記號，勢必會拖垮網路的整體速度，目前我們最新的想法是，我們將每一台電腦設定一個時間週期，進而去比較每一台電腦所發送的 ARP 封包，如果哪一台 ARP 的封包發送的量高低不均頗為異常，將它列入工機主機的名單內，不過這只是草創階段，還有很多東西都是很模糊的，像是時間週期的長短要如何定義，因為欺騙位置解析協定攻擊（ARP Spoofing Attack），只要短短的數秒就能癱瘓使用者的電腦，如果寫成常駐程式那電腦的資源運用和其他種種的問題便油然而生，如果使用 ICMP 協定，那勢必線至區域網路內的節點 (node)都必須開起這一個通訊協定，那是否會造成另一種危機，網際網路控制訊息協定欺騙攻擊 (ICMP Spoofing Attack) 這些課題都是我們將來努力的方向。

參考文獻

[1] Request For Comments: 826

[2] Request For Comments: 792

[3] 劉修仁，在交換式乙太區域網路中防範封包監聽之研究，義守大學資訊工程研究所碩士論文，2003。

[4] Computer Foundation，http://www.study-area.org/study.old/network/network_arp.htm。

[5] 常見網路監聽手法分析與防護策略，http://blog.no99.idv.tw/print.php?articleId=157&blogId=2。

[6] 陳年興，台灣電腦網路危機處理中心通訊第七十四期，2004/12。

[7] TWCERT/CC 台灣電腦網路危機處理暨協調中，http://www.cert.org.tw/index.php。

[8] Pank's Blog: Notes Archives，http://pank.org/blog/archives/cat_notes.html。

[9] Behrouz A. Forouzan, Sophia Chung Fegan 原著，陳中和、吳秀峰翻譯，TCP/IP 協定，2003。

[10] Andrew S.Tanenbaum 原著，蔡明智翻譯，電腦網路，1998。

[11] 資訊安全課程，http://www.chu.edu.tw/~jerry/infosec/。

[12] 弱點資料庫，http://vdb.dragonsoft.com.tw/。

[13] 網路安全資訊論壇，http://www.all4u2c.net/crack/index.php。

[14] CRETIX Security, http://www.hacker.org.tw/。

[15] 安全物語, http://www.securitytalk.net/。

[16] 國家資通安全會報技術服務中心，http://www.icst.org.tw/。