Address Resolution Protocol(ARP)攻擊之手法與防範對策之模擬與研究

期間:96年9月16日至97年4月30日

電機三甲 林宮漢　陳文笙　蕭一凡

一、 背景

在廣大無疆的網際網路世界裡,潛藏了許許多多的危機,但也由於資安設備技術進步有效的阻隔了大多數外在攻擊,而雖然如此,由於IT使用習慣的改變及入侵與病毒的傳播技術日新月異,近年來的資訊及網路安全威脅開始來自於企業infrastrunture內部。2007 舊金山 RSA conference 正說明了這一點,會中一致的共識說明「單純的單點防禦,或是築起一道堅固的資訊防禦外牆,已經逐漸不能滿足企業(機関)在資訊安全上的需求,取而代之的,未來企業(機関)越來越需要整體內部網路與系統的協同防禦機制。」為何ARP欺騙攻擊是現階段病毒攻擊網路最喜歡的攻擊工具,也是現階段駭客最喜歡使用的入侵工具之一,有了這些了解後,網路管理者將可更有效佈署或整合適當的網路與資訊安全設備,檢測出網路與資訊威脅來源。

1.1何謂ARP欺騙 ?

ARP Spoofing（ARP 欺騙）攻擊的根本原理是因為 Windows 電腦中維護著一個 ARP 快取記憶體（讓你可以使用 arp 命令來查看你自己的 ARP 快取記憶體），並且這個 ARP 快取記憶體是隨著電腦不斷的發出 ARP 請求和收到 ARP 回應而不斷的更新的， ARP 快取記憶體的目的是把機器的 IP 位址和 MAC 位址相互映射，使得 IP 資料包在乙太網內得順利而正確找到目的 MAC 位址，然後正確無誤的傳送。如果你可以藉由發出標準的 ARP 請求或 ARP 回應來擾亂或竄改某電腦或路由器內正常的 ARP 表，而導致該電腦(或路由器)發出的資料包誤傳目的地，或使 OSI 的第二層乙太網和第三層無法連接，進而癱瘓網路，我們就稱你使用了 ARP 欺騙攻擊。

舉例說明： 現在有三部機器分別是機器 A：IP1/MAC1、機器 B：IP2/MAC2、機器 C：IP3/MAC3。現在機器 B 上的用戶是位駭客企圖干擾機器 A 或是監視 SNIFFER 機器 A 與 C 之間的通訊，首先他向機器 A 發出一個 ARP Reply，其中的目的 IP 位址為 IP1，目的(Destination) MAC 位址為 MAC1，而源(Source)IP 地址為 IP3，源 MAC 地址為 MAC2 。好了， 現在機器 A 更新了他的 ARP 快取記憶體，並相信了 IP3 地址的機器的 MAC 地址是 MAC2 。當機器 A 上的管理員發出一條 FTP 命令時---ftp IP3，資料包被送到了 Switch，Switch 查看資料包中的目的地址，發現 MAC 為 MAC2 ，於是，他把資料包發到了機器 B 上，因此成功攻擊機器 A。現在如果不想影響 A 和 C 之間的通信該怎麼辦？僅是 sniffer 監視兩者之間的通訊，你可以同時欺騙他們雙方，使用 man-in-middle 攻擊，便可以達到效果 。

總之本機在傳送資料包之前，會送出一個關於查詢目的 IP 位址的 MAC 乙太網廣播包。正常情況下，只有對應目的 IP 的主機會以一個自己的 48 位元 MAC 主機位址 unicast 包來做回應，並且將該 IP 與 MAC 位址對應更新本機內 ARP 快取記憶體，以節約不必要的 ARP 通信。如果有一個中毒的電腦或是網內合法授權進行非法活動的駭客，他們是對本地網路具有寫訪問許可權，極可能這樣一台機器就會發佈虛假的 ARP 請求或回應通訊，欺騙其他電腦或路由器將所有通信都轉向它自己，然後它就可以扮演某些機器，或對資料流程進行修改。這樣就造成 arp 欺騙攻擊，影響正常的主機通信。

二、 ARP欺騙造成的結果

2.1 ARP欺騙被使用的目的為何? 它攻擊的特色為何?

不管是中毒無特定目標的攻擊或是駭客進行特定標的非法監聽、竊取活動，ARP欺騙是主要攻擊的一種手法也是目的。事實上很多的知名的駭客使用的工具就是使用ARP欺騙為手法的。最有名駭客攻擊的手法如中間人攻擊(Man-in-the-Middle attack) 與連線劫奪(Session Hijacking) 就是採取ARP spoofing等攻擊手法達到欺騙主機、反追蹤或是避開交換器訪問安全存取的安全機制的防護。連線劫奪(Session Hijacking) 利用ARP欺騙將使用者正常的連線搶過來;中間人攻擊則利用ARP同時欺騙使用者(Client)與服務器(Server)兩邊使所有兩邊的交談都要透過入侵人的轉述，達到欺騙、側錄、竄改資料的目的。

另外中毒的電腦發送 ARP 欺騙封包，或是市面上也有些軟體如網路剪刀手（NetCut），利用製造 ARP 欺騙封包，它則是以攻擊為目的，使得特定或不特定的目標癱瘓，並嫁禍於人。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，將錯誤的實體網路位址（MAC）記到 ARP 表內，伺服端（Client）的返回封包就無法送達，也就無法上網，達到攻擊的目的。

ARP 欺騙手法最大的特色是隱密難以偵測，和過去駭客或中毒攻擊手法 - DsS 攻擊或洪水攻擊(Flooding)不同，DoS 或洪水攻擊所造成的網路危害明顯，但是容易被查覺；而 ARP 欺騙則是以欺騙為目的，並且為了維持持續的欺騙效果，必須持續發送 ARP 欺騙包，這些 ARP 欺騙包長度短但是為數可能頗多，因此造成的網路危害不僅是可能的資料側錄、竊取，也可以是對網路特定目標的攻擊，甚至大量 ARP 廣播包也可造成整個或部份網路的癱瘓。

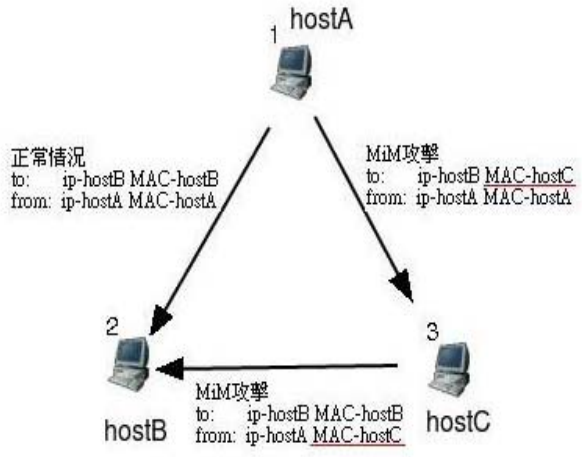
2.2 ARP攻擊分類、手法；
為何網路管理員難以辨識及防禦 ARP的攻擊？

ARP欺騙攻擊分類基本上可以分為刻意的特定目標攻擊，及因為中毒無意的攻擊。這二種的攻擊本意有所不同，(一)通常是利用網路下載的工具、例如網路翦刀手netcut程式 然後惡意攻擊他人並將攻擊封包偽裝以嫁禍於他人，其危害常是少數特定目標，但是由於攻擊者以Unicast 包方式傳送且善於偽裝，因此網路管理員極難找出問題所在，也由於此類型程式下載容易操作簡單，近期於網路中快速擴散，造成網路管理人員極大負擔，也由於目前尚無完整機制快速偵測出此類型規則來源，因此常會使管理人員處理此類問題時疲於奔命，處理耗費時間同時效果不彰，過程中也讓網路管理人員專業能力受到極大的質疑。

〈二〉通常是使用者中毒後中毒軟體發送ARP欺騙封包以誤導其他人將封包送往錯誤的路徑,導致變像的攻擊使閘道受害或某用戶的遭炔,其主要的目的是造成部份或整體網路的危害 。

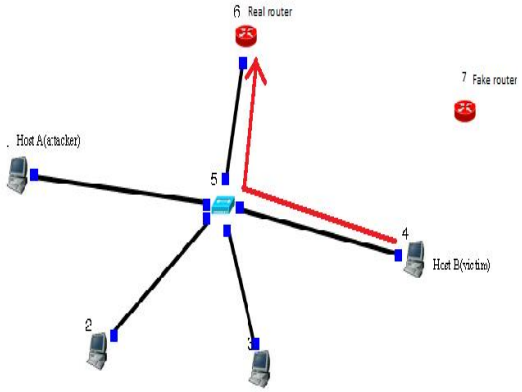
就一般來說現在的攻擊方式具體而言有

1. ARP 緩衝溢位攻擊(建立在同一區網中)[1]：駭客丟大量的封包，使得受害者的 ARP 緩衝區無法在同一時間處理量資料進而癱瘓。
2. Host 扮演[1]：駭客把路由器的 ARP 表中的被害者的 IP MAC 改成自己的 IP MAC ，同時也把被害者的 ARP 表中的路由器 IP MAC 位置改成駭客自己的 IP MAC，這樣一來使得駭客可以輕而易舉獲取被害者的資料。
3. MIM 攻擊[1]：在兩個主機之間的通訊，更改自己的位址讓資料物傳到自己的主機上。

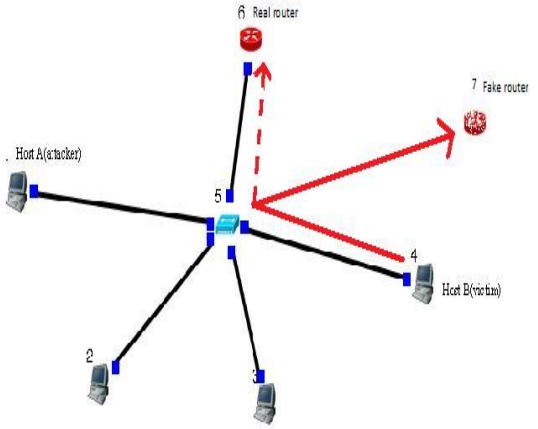


4. Cloning 攻擊(MAC的欺騙攻擊)[1]：駭客把被害者所得到的路由器IP MAC 改成被假的IP MAC，使得被害者傳送資料都是往甲的位置傳送會導致 Dos 還有網路斷線。

攻擊前



攻擊後

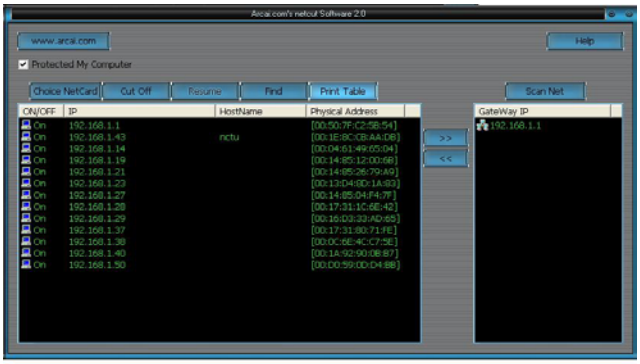


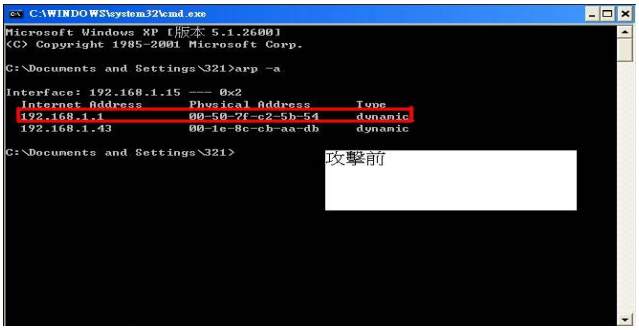
5. port stealing 攻擊[2]：駭客在 LAN 中發送一個假的 MAC 位置，傳送給 switch 而且 MAC 對應的 IP 位置是沒有人在使用的，這樣來填塞 switch 的 Port-Mapping Table，導致尚未紀錄在 switch 中的使用者無法順利進行網路連線。

位置解析協定（Address Resolution Protocol）在區域網路中極其重要，他是屬於區域網路同一子網段內部主機對主機的傳輸或主機與路由器之間傳輸重要的協定。如果局域網內是屬於中大型網路具有多個子網路，那麼防火牆/IPS 入侵偵測設備通常被設置在核心路由交換器之後根本沒有機會接觸 ARP 封包，因此對 ARP 攻擊束手無策。即使局域網內只有一個網段，防火牆/IPS 入侵偵測設備兼具路由器功能也僅能偵測部分 ARP 廣播包，且大部分的產品如使用作業系統(如 Linux)的 TCP/IP Socket 就難以偵測 ARP 數據包，因此目前的防火牆/IPS 入侵偵測設備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，就算有也僅止於出口控制無法由網路底層第一時間阻隔此類攻擊。

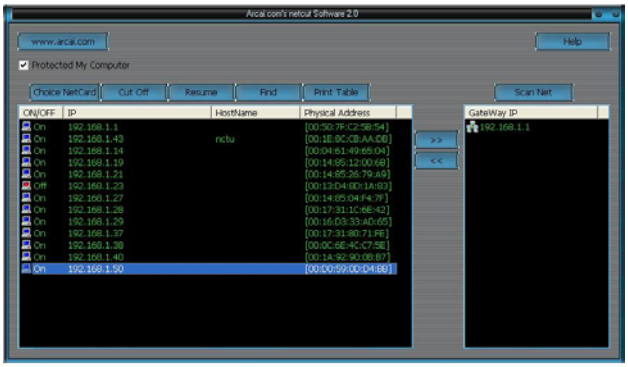
6. 以 NETCUT 示範簡單 ARP 欺騙，以造成目的電腦網路斷線 。

攻擊前

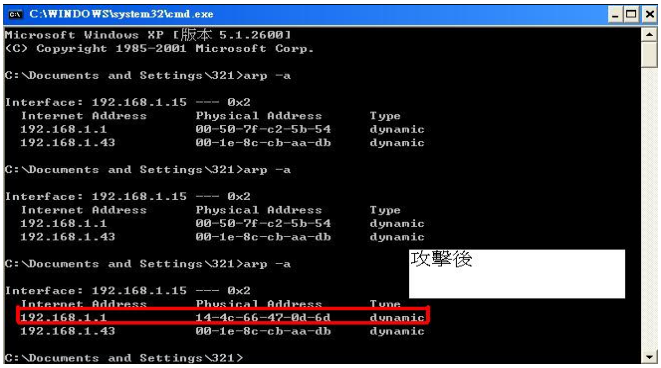




攻擊後 (攻擊 192.168.1.23)



被攻擊者(192.168.1.23) 的 Gate Way (192.168.1.1)Mac Address 已被改變



三、防範方法

目前我們整理出各種不同的防範方法

Itrusion Detection Systems(IDSs 攻擊發現系統)

ex:Snort[3]：它會產生大量的 false positive，但它偵測到的 ARP 病毒是有限的，無法防堵全部的 ARP 攻擊類型。

Carnut et al.[4]：提出一種結構可以找出 ARP 的欺騙，它沒有大量的 false positive，但是有缺點就是 ARP 攻擊多半隱藏在大量流量之中，在相當長的一段期間也依然無法偵測到攻擊。 引用 ARP-Guard[5]:他利用 sensor-based 的一種結構去偵測和當地內部網路中的各種網路攻擊，當這個管理系統從 LAN 和 SNMP 感應器收到資料去分析之後，ARP 攻擊被偵測到時系統會發出警報給管理者。

Clonong attack[6] ：可以用 port security 來預防。雖然非常有效但是對於假冒 MAC address 就無法預防。[13]

Tripunitara et al[7]：提出利用電腦中介軟體的角度切入非同步、和 backward compatible 來察覺和防範 ARP 緩存區被正面攻擊。這個方法無法防範當惡意的主機匿名時候的攻擊或者是 DoSed 攻擊 。

SARP[8]是一個向後相容(backward compatible)延伸的部分，ARP 可以信任在 public-key 的密碼去認證 ARP 的回應，這個解決辦法是應用在 LAN 中，每個 host 將原來的 ARP 加密改成 SARP。此外 host 必須要有認證的權利，稱做 AKD，它是一個可以隨時聯繫得到另一個 host 的 public key 的機制，所以 host 的回應可以被認證並且加上記號。AKD 也可以區分它的計時值(TTL)，所以其他的 host 可以同時執行這個動作。它可以去防範回應的攻擊，像是欺騙 host 的攻擊(或是 DoS 攻擊)。這個系統是建立在 Linux 上，用一個動態的 IP 任務去做一個相符的解決辦法，一個修正過的 DHCP 稱做 S-DHCP 的概念就被提出來。 這個計畫的缺點在網路中 AKD 的結構若出了問題，host 就不能進行檢驗未知 host 的 ARP 封包(i.e 傳送者的 public key 不會傳到接收的 key ring)，甚至 AKD 正常工作下，攻擊者可以複製 host 的 MAC 位址去扮演一個 host(但是要直到將 host 中的緩存表也一起複製，在 host 正在攻擊時)。

TARP[9]利用分發的中心發佈一個安全的<IP MAC>位址經由存在的 ARP 訊息來 mapping 認證(稱做 tickets)。這些 tickets 是從中心所產生的和經由 Local Ticket Agent(LTA)去標記，tickets 包含著結束的時間(timeout)。hosts 在這些 ARP 回應會附上 tickets，接收者可以去確認這些合法的位址與 tickets。TARP 是向後相容(backward compatible)的 ARP，SARP 是容易經由 small windows 的弱點受到回應攻擊所影響。這是在 Linux 上去執行 TARP，在一個結合核心模組和使用者空間 daemon。

Goyal et al. [10]被推舉出一種 SARP 的新的結構。這個系統建立在 Merkle hash tree，在網路中一個可以被信任的節點 trusted node(TN)和一個廣播認證的協定(e.g. Tesla)。這個解決辦法有優點，它不需要 對稱/不對稱的密碼運作模式。並且有一個方法[雜湊函數]hash functions(它是出名的被用來計算速度的 function)被使用。如果 TN 已經損壞但 host 還是可以繼續工作。當一個新的 host 增加到網路中時 TN 是必須存在的，或是<IP,MAC>被改變時 TN 必須存在。在這情況中，TN 會再次計算 hash tree 和區別出新加入的 host 與其他 host。他最主要的缺點是它與 ARP 沒有向後相容(backward compatible)和當它在高流動率的網路中是非常沒有效率的。

Goyal et al. [11]提出一個修改 S-ARP 的方法建立在結合數位簽章(digital signature)與先前所用的密碼，它們可以利用 hash chain 去使 ARP<IP,MAC>mapping 生效。這是建立在相同的 S-ARP 結構中，它是巧妙的使用密碼去讓它執行得更快速。

有些較高檔的 Cisco switch 有一個新的功能稱作[動態 ARP 檢查]Dynamic ARP Inspection [12]。這個功能允許 switch 去擷取內容是無用的<IP,MAC>位址的 ARP 封包[13]。可以去偵測有無用的<IP,MAC>位址的 ARP 封包，switch 利用一個當地的<IP,MAC>表去建立，利用這個功能的結構稱作 DHCP snooping。這個機制可以保證是一個非常有效率的方法去解決 ARP 攻擊，但是經過測試，它需要被執行確認的動作，它是一個可以去預防所有的 ARP 攻擊方法。這個解決方法有一個主要不利的條件就是這個 switch 是高成本的(high cost)。此外它是依賴在 DHCP sever 和網

路的結構中，在 VLAN 中它可能不會使一些 ARP 封包在 switch 中產生效用[8]。

四、討論

基本預防或是阻擋 ARP 攻擊的構思
有一個簡單又有效的方法去預防 ARP 攻擊，就是利用在 ARP 緩存區狀態設成 static[1]，這個方法有兩個缺點:
(1)它不能工作在 dynamic 的環境中
(e.g.network 是使用 DHCP(Dynamic Host Configuration Protocol))
(2)當網路的管理者在部屬整個網路以及將新的 table 上傳時，這對網路的管理者來說它會變得很難處理。
但是有些作業系統(像是 Windows)可以接受 dynamic ARP 回應和上傳 static entry[14]網路是個開放空間所以他需要的是靈活的環境，所以我們更需要討論出有效的方法來防範 ARP 攻擊 。
整體而言的 ARP 攻擊可分為幾種類型 ：

一.廣播攻擊(主要目的在於讓讓受害者網路癱瘓)

1.攻擊者有更改自己的 MAC 和 IP，在進行攻擊。

2.攻擊者沒有更動自己得 IP 和 MAC，便進行攻擊。

二.MIN 攻擊(主要目的在於竊取受害者的資料)

當一台電腦要開始連線請求的時候他會請求 router 給他一個 IP 位置，所以我們大膽推測 host 在一開始取得的 IP(router)位置會是正確的，否則他無法拿到正確的 IP 做網路連線。因此如果要對 host 進行欺騙攻擊把假的 router IP 給 host，並且也會對真正的 router 作欺騙讓 reouter 把原本要送到 host 的資料先送到駭客那邊，如此一來就完成了 竊取資料的程序。只要在 host 端的 ARP table 不在做更換，駭客就無法成功欺騙 host 了，即使駭客成功的欺騙了 router 這樣一來當 host 沒有接受到他的封包就會發現有人在竊取他的資料。以上次針對 MIN 攻擊做更進一階的討論，好讓我們可以討論出更棒的防範方法。

如果駭客要進行廣播攻擊，假設他沒有更改自己的 IP 就開始發動攻擊，這樣一來不管是 host 或者是 router 只要發現同一個 IP MAC 不停的在發送封包企圖照成網路癱瘓，只要確實的知道誰在惡意攻擊就可以直接封鎖他的 IP MAC 封包，使得他無法作亂。但是駭客不會這麼笨，它們會更動自己真實的 IP MAC 使得每一次的廣播封包都是不同的 IP MAC 而且沒有一組是真的，使得 router 或者是 host 端都無法正確的把惡意的 host 封鎖，也會間接造成 DOS 攻擊，因此這類型的攻擊最麻煩防範。

但是就這兩大類的攻擊我們可以把反制措施設定在 host 上或者是 router 上， 如果在 host 端可以有效的防範 MIN 攻擊但是對於廣播攻擊則要再想有效的方法防範，反之如果在 router 上就可以有效的防範所有 ARP 的攻擊，但是建構在 router 的成本太貴。

五、結語&展望

一.當 ARP 加上 DoS 是最麻煩且最難防範的攻擊我們發現雙向綁定是最有效的防治 ARP 攻擊的方法，但是當區網內如有不在上網的 host 端，那麼一開始分配的 IP 便會成為幽靈 IP，要解這個問題只能有管理者去一一檢查，所以雙向綁定會造成管理者的龐大負擔，於是我們討論出一種防範方法，界在 host 和 router 兩端，在 router 的部分多加入一種確認機制，也就是說每當區網內有 host 端需要連線時，便須向 router 端送出一"連線請求"，這時 router 端便會回 ping 這個請求，只要是真的來源端，便會回傳此 ping 給 router，這時雙向綁定連線便建立；當 host 端，要離開網路時必須送出一"請求中斷"的要求，這時 router 端收到"請求"便會中斷連線 ；當 host 端沒有經此正常程序就斷線，route 便會封鎖此 MAC address ；如此一來可以解決在雙向綁定中須由管理者去一一檢查 IP PORT 的麻煩，且可解決 MIM 的 ARP 欺騙。 而此"連線"，"中斷"請求可經由軟體安裝在 host 端，當 host 端須建立連線時便須啟動此軟體(稱此軟體為 ARP 剋星，會常駐直到中斷連線為此,如被關掉或關機便會傳送中斷請求。)當 ARP 剋星啟動後便抓取此 host 端的 MAC address ，當 host 端經由 ARP 剋 星送出連線請求時，便會先比對此封包內的 MAC address 與實際的 MAC address 符不符合,如符合便會送出一加密封包給 router 端,讓 router 通過此"連線請求",如不符合便會在 host

端先擋住此封包，並傳送一加密封包給 router 端，讓 router 封鎖此 MAC address，如此一來既可避免 ARP 欺騙且可防治變相 DoS 攻擊，且可達到雙向綁定的功用，並且不造成管理者的龐大負擔，另外 ARP 剋星就像是 ARP 防火牆一樣，且經由特殊加密傳送的封包,可避免被駭客假造此"請求封包"，當然 Router 端所接收的"請求封包"，也非此加密不可。