ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1998
Seria: INFORMATYKA z. 34 Nr kol. 1381

Igor BOKUN
Akademia Górniczo-Hutnicza, Katedra Informatyki

[1]PROTOKÓŁ ARP JAKO ŹRÓDŁO ZAGROŻENIA BEZPIECZEŃSTWA LOKALNEJ SIECI KOMPUTEROWEJ

Streszczenie. Protokół ARP jest jednym z podstawowych elementów składowych sieci TCP/IP zapewniającym odwzorowanie adresu IP na adres MAC. Niniejszy artykuł ukazuje, iż protokół ten może być źródłem poważnego zagrożenia zarówno tradycyjnej sieci LAN, jak i lokalnej sieci komputerowej zbudowanej w oparciu o urządzenia bridge lub switch LAN.

SECURITY WEAKNESS OF THE ADDRESS RESOLUTION PROTOCOL

Summary. ARP is the fundamental part of the TCP/IP protocol suite. It provides mapping between an IP and hardware address. This paper describes a security weakness of the ARP which can lead to the degradation of security level in traditional, shared LAN as well as the micro-segmented network based on the LAN switches or bridges.

1. Wstęp

Dynamiczny rozwój sieci komputerowych, którego jesteśmy świadkami w ostatnich latach, powoduje wzrost zainteresowania zagadnieniami bezpieczeństwa systemów komputerowych. W epoce, w której wiele transakcji handlowych przeprowadzanych jest za pośrednictwem sieci komputerowych, poufność danych czy też możliwość jednoznacznej identyfikacji osoby zawierającej transakcję staje się pierwszoplanowym problemem.

[1] Artykuł opracowano w ramach grantu KBN nr 8T11C01210

Mimo wzrostu znaczenia bezpieczeństwa sieci komputerowych obserwujemy niepokojąco wiele sygnałów o wykryciu luk bezpieczeństwa w powszechnie stosowanych, komercyjnych systemach komputerowych.

W niniejszym opracowaniu przedstawiona zostanie poważna luka w bezpieczeństwie sieci komputerowej, związana ze stosowaniem protokołu ARP. Wykorzystując opisywaną technikę potencjalny intruz jest w stanie zmienić trasę pakietów przesyłanych w sieci, jak również doprowadzić do zmiany zawartości pakietów.

W rozdziale 2 został zdefiniowany zakres opisywanego zagrożenia. Rozdział 3 zawiera podstawowe informacje na temat działania urządzenia switch. W rozdziale 4 przedstawiono protokół ARP. Rozdział 5 zawiera szczegółowy opis ataku wykorzystującego luki bezpieczeństwa protokołu ARP. Rozdział 6 poświęcono metodom zapobiegania tego rodzaju atakom. W ostatnim rozdziale zawarto ogólne podsumowanie przedstawianego problemu.

2. Zasięg opisywanego zagrożenia

Przedstawiana w niniejszym artykule metoda wymaga fizycznego dostępu do sieci komputerowej. Ogranicza to w dużym stopniu jej zasięg stosowania. Pakiety protokołu ARP, umiejscowionego w warstwie łącza danych, nie są przesyłane przez urządzenia typu router. Można więc stwierdzić, iż router określa granicę stosowania omawianej techniki.

W praktyce często stosuje się segmentację sieci komputerowej za pomocą urządzeń typu bridge czy też switch LAN. Te urządzenia, jako że operują na warstwie łącza danych, nie stanowią zapory dla przedstawianej techniki. Oznacza to, że intruz jest w stanie dokonać ataku na segment sieci, który jest odseparowany od dostępnego mu segmentu jednym lub wieloma urządzeniami typu bridge lub switch.

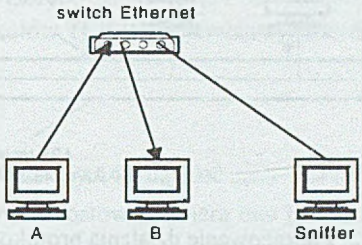
Ze względu na duże podobieństwo pomiędzy logiką działania urządzeń switch oraz bridge w dalszej części artykułu uwaga zostanie skupiona na jednym z nich - switchu.

3. Zasada działania switcha Ethernet

Switch Ethernet jest urządzeniem umożliwiającym przełączanie pakietów na poziomie warstwy łącza danych modelu odniesienia OSI. Posiada on pewną ilość portów, do których można podłączać zarówno pojedyncze urządzenia, jak i segmenty sieci. W odróżnieniu od urządzenia hub switch nie rozsyła otrzymanego pakietu na wszystkie swoje porty. Switch podejmuje decyzję o skierowaniu pakietu na konkretny port na podstawie adresu przeznaczenia danego pakietu. Proces ten musi być poprzedzony fazą adaptacji (uczenia się) switcha, który

na podstawie adresów źródłowych pakietów kojarzy interfejs sieciowy z numerem portu. Pakiety braodcast oraz multicast rozsyłane są na wszystkie porty switcha.

Przedstawione cechy umożliwiają zwiększenie wydajności sieci komputerowej Ethernet poprzez zmniejszenie tzw. domeny kolizji. Jednocześnie właściwości switcha umożliwiają wykorzystanie go jako urządzenia zwiększającego bezpieczeństwo sieci komputerowej, co zostało zobrazowane na poniższym rysunku.



Rys. 1. Switch jako zapora przed pasywnym sniffingiem
Fig. 1. LAN switch as a protection from passive sniffing

W przedstawionym przykładzie do switcha podłączone są trzy urządzenia. Pomiędzy komputerami A i B przesyłane są pakiety IP odpowiadające bądź interaktywnej sesji *telnet*, sesji *ftp* czy też innej dowolnej usługi opartej na protokole IP. Mimo zainstalowania odpowiedniego oprogramowania na maszynie Sniffer potencjalny intruz nie ma możliwości podejrzenia przesyłanych pakietów pomiędzy A i B. Wyjątek stanowią pakiety rozgłoszeniowe oraz multicastowe, przesyłane na wszystkie porty switcha. Pakiety te zwykle nie przenoszą istotnych informacji, takich jak na przykład hasła dostępu do systemu.

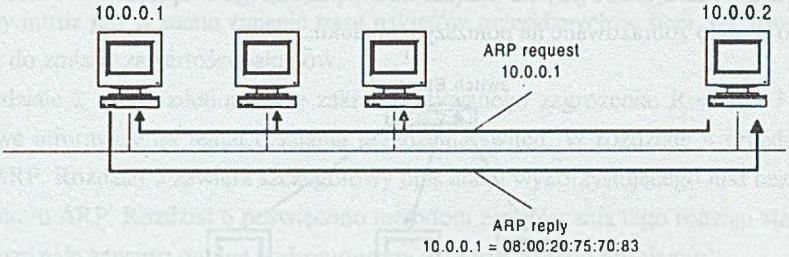
Dla porównania zastosowanie urządzenia hub umożliwia intruzowi obserwację całego ruchu w danym segmencie sieci.

Niniejszy artykuł ukazuje, iż jakkolwiek switch stanowi ochronę przed klasycznym, pasywnym sniffingiem, dodanie do procesu podsłuchiwania sieci czynnika aktywnego umożliwia intruzowi podsłuchanie pakietów IP kierowanych na inne porty switcha.

4. Podstawowe informacje o protokole ARP

Interfejsy sieciowe w powszechnie stosowanych sieciach Ethernet podejmują decyzję o przyjęciu lub odrzuceniu pakietu na podstawie 48-bitowego adresu sprzętowego zawartego w polu destination pakietu. Zadaniem protokołu ARP (Address Resolution Protocol) jest odwzorowanie logicznego adresu IP na adres sprzętowy, w szczególności adres Ethernet. Oficjalna specyfikacja protokołu ARP zawarta jest w [4].

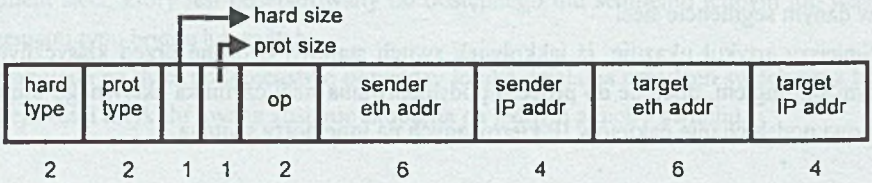
Ideę działania protokołu ARP przedstawiono na rysunku 2. W przedstawionym przykładzie komputer o adresie IP 10.0.0.2 rozpoczyna komunikację na poziomie IP z komputerem o adresie 10.0.0.1.



Rys. 2. Zobrazowanie działania protokołu ARP
Fig. 2. The idea of the Address Resolution Protocol

W celu uzyskania adresu sprzętowego skojarzonego z logicznym adresem IP komputer 10.0.0.2 wysyła pakiet ARP request o adresie rozgłoszeniowym równym FF:FF:FF:FF:FF:FF. Pakiet ten dociera do wszystkich interfejsów sieciowych w danym segmencie sieci. Tylko jeden komputer, ten o adresie IP równym 10.0.0.1, odpowie na zapytanie. W celu uniknięcia nieskończonej pętli zapytań ARP w pakiecie request zawarty jest zarówno adres IP, jak i adres sprzętowy komputera wysyłającego zapytanie. Dzięki temu odpowiedź może być wysłana do odpowiedniego interfejsu sieciowego.

Struktura pakietu ARP została przedstawiona na rysunku 3.



Rys. 3. Struktua pakietu ARP
Fig. 3. ARP packet format

Pakiet ARP poprzedzony jest standardowym nagłówkiem Ethernet lub też nagłówkiem zgodnym ze specyfikacją 802.2.

Pole hard type określa typ adresu sprzętowego. W przypadku sieci Ethernet pole to ma wartość 1. Pole prot type określa typ protokołu warstwy sieciowej i wynosi dla protokołu IP 0x0800. Kolejne dwa pola, hard size i prot size, określają odpowiednio długość adresu sprzętowego oraz adresu logicznego. W omawianym przypadku polom tym przypisane są odpo-

wiednio wartości 6 i 4. Kolejne, dwubajtowe pole określa rodzaj pakietu. Wartość 1 zarezerwowana jest dla zapytania ARP (ARP request), natomiast wartość 2 dla odpowiedzi (ARP reply). Pozostałe wartości tego pola zarezerwowane są dla protokołu RARP. Następne pola zawierają adres sprzętowy oraz adres IP komputera wysyłającego zapytanie oraz identyczną parę adresów komputera, dla którego przeznaczony jest pakiet.

ARP jest jednym z nielicznych protokołów z rodziny TCP/IP stosującym adresy rozgłoszeniowe. Wykorzystywanie stosunkowo niewielkiej ilości pakietów rozgłoszeniowych jest uważane za dużą zaletę protokołów TCP/IP, pozwalającą na budowanie dużych sieci.

4.1. Cache ARP

Istotnym czynnikiem zwiększającym wydajność sieci TCP/IP jest pamięć cache protokołu ARP umiejscowiona na każdym z hostów. Zawiera ona powiązania pomiędzy adresami IP a adresami sprzętowymi tych komputerów, z którymi dany komputer wcześniej się komunikował. Elementy pamięci cache ARP utrzymują swoją ważność przez okres od kilku do kilkunastu minut w zależności od konkretnej implementacji systemu. Po upływie tego czasu podsystem TCP/IP ponownie wysyła zapytanie ARP. Umożliwia to sprawną pracę sieci nawet wtedy, gdy w którymś z hostów zostanie wymieniony interfejs sieciowy, co spowoduje zmianę adresu sprzętowego.

Zawartość pamięci cache ARP można wyświetlić wydając następujące polecenie:

```
$ arp -a
```

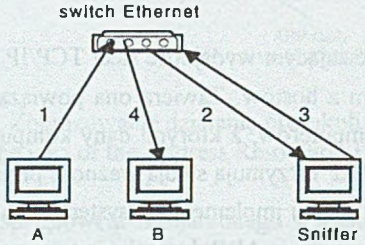
W celu optymalizacji wydajności sieci wpisy do pamięci cache protokołu ARP aktualizowane są również po odebraniu pakietów ARP request. Pakiety te są pakietami rozgłoszeniowymi, zatem trafiają do wszystkich interfejsów sieciowych w danym segmencie sieci. Zawierają one zarówno adres sprzętowy, jak i adres logiczny interfejsu wysyłającego zapytanie. Pozwala to na aktualizację wpisu do pamięci cache. Należy zauważyć jednak, że odbiór pakietu ARP request nie spowoduje dodania nowego wpisu, jeśli takowy nie istniał, a jedynie aktualizację istniejącego już wpisu.

5. Atak z wykorzystaniem protokołu ARP

Termin ARP spoofing oznacza umieszczanie w polach pakietów ARP nieprawdziwych adresów. Umożliwia to podszywanie się pod inny komputer w sieci lub też zmianę skojarzenia adresu sprzętowego z adresem logicznym IP. Protokół ARP jest szczególnie podatny na takie działanie ze względu na swój bezpołączeniowy, datagramowy charakter.

W przedstawianej metodzie ataku wykorzystano fakt akceptowania przez hosty dowolnych pakietów ARP reply, mimo iż wcześniej nie wysyłały one odpowiednich pakietów ARP request. Zachowanie takie jest dość powszechne we współczesnych systemach operacyjnych. Oznacza to, iż odpowiednio preparując pakiety ARP reply potencjalny intruz jest w stanie dowolnie zmienić skojarzenie adresu IP z adresem sprzętowym.

Przedstawiona cecha protokołu ARP umożliwia przeprowadzenie ataku typu „packet path redirection". Ataki tego typu polegają na zmianie trasy pakietu dokonanej przez intruza. W przedstawianym przykładzie głównym celem zmiany trasy pakietu jest skierowanie go na port switcha, na którym zainstalowane jest oprogramowanie podsłuchujące ruch sieci.



Rys. 4. Zmiana drogi pakietów
Fig. 4. Packet path redirection

Rysunek 4 przedstawia ideę opisywanej metody ataku. Intruz modyfikuje trasę pakietów IP wysyłanych z komputera A do B, tak by zostały one skierowane na ten port switcha, na którym intruz zainstalował oprogramowanie podsłuchujące ruch w sieci. Intruz musi po odebraniu pakietu przeznaczonego dla maszyny B odesłać pakiet do jego prawdziwego adresata, tak by nie zostało przerwane logiczne połączenie pomiędzy A i B. Oczywiście analogiczne czynności przeprowadzane są w przypadku pakietów IP skierowanych z komputera B do A.

5.1. Zmiana drogi pakietów IP

W przedstawionej metodzie ataku zmiana drogi pakietów realizowana jest przez wysyłanie w regularnych odstępach czasu pakietów ARP reply zawierających nieprawdziwe skojarzenie adresu IP z adresem sprzętowym. Wracając do poprzednich przykładów, intruz wysyła dwa pakiety ARP reply:

1.skierowany do komputera A, zawierający informację, że adres IP komputera B przypisany jest do interfejsu sieciowego komputera Sniffer,

2.skierowany do komputera B, zawierający informację, że adres IP komputera A przypisany jest również do interfejsu sieciowego komputera Sniffer.

Z punktu widzenia sieci TCP/IP sytuacja, w której jeden interfejs sieciowy posiada kilka skojarzonych adresów IP, jest całkiem poprawna.

Odbiór pakietów ARP reply przez stacje A i B powoduje natychmiastową zmianę w pamięci cache protokołu ARP i wszystkie pakiety zostaną od tej pory przesłane pod inny adres sprzętowy, co spowoduje ich jednoczesne skierowanie na inny port switcha. Dodatkowo wysyłane pakiety ARP reply spowodują aktualizację wewnętrznych struktur switcha, przez co będzie on miał informację o tym, do którego portu podłączony jest komputer Sniffer.

Ważną cechą przedstawionej metody jest całkowita przezroczystość dla potencjalnej ofiary ataku. Metoda ta jest skuteczna zarówno przed nawiązaniem połączenia przez komputery A i B, jak również w czasie trwania połączenia.

5.2. Rozsyłanie pakietów

Po wykonaniu przedstawionych czynności zarówno pakiety przeznaczone dla komputera A, jak i te dla komputera B trafią do komputera intruza. Aby nie doprowadzić do utraty pakietów oraz do przerwania połączenia, intruz musi z powrotem odesłać pakiety, by trafiły one do rzeczywistych adresatów. Czynność ta polega na prostym forwardingu pakietów bazując na ich faktycznych adresach sprzętowych, które intruz wcześniej zapamiętał. Ze względu na zmianę jedynie nagłówka Ethernet pakietów nie jest konieczne ponowne obliczanie sum kontrolnych IP czy też protokołów wyższych warstw.

5.3. Cechy przedstawianego rodzaju ataku

Aby istniała możliwość przeprowadzenia opisywanego ataku, konieczne jest spełnienie następujących warunków:

- Intruz musi mieć możliwość odbioru i generowania pakietów Ethernet na poziomie warstwy łącza danych.
- Zarówno komputery atakowane, jak i komputer używany przez intruza muszą znajdować się w tej samej sieci.
- W atakowanej sieci musi być wykorzystywany protokół ARP.
- Komputery atakowane muszą być nieodporne na ARP spoofing. W praktyce dotyczy to wielu popularnych systemów operacyjnych. Potwierdzają to testy przeprowadzone przez autora w następujących środowiskach:
- DOS ze stosem Waterloo TCP/IP.
- Windows 3.X, Windows 95, Windows NT.
- Linux.
- SunOS.

6. Metody zapobiegania

Zasadniczym czynnikiem umożliwiającym przeprowadzenie opisywanego ataku, jak i wielu innych, jest możliwość dostępu przez intruza do sieci na niskim poziomie - warstwy łącza danych. W przypadku systemów DOS, Windows 3.x czy też Windows 95 każdy użytkownik systemu ma możliwość wysłania i odbioru pakietów na poziomie warstwy łącza danych.

W systemach UNIX, w tym również w systemie Linux, tworzenie i wysyłanie dowolnie spreparowanych pakietów jest również możliwe, wymaga jednak uprawnień użytkownika root.

W przypadku sieci, w których z pewnych względów pracują wymienione wcześniej systemy operacyjne, należy przeanalizować następujące zagadnienia:

1. Jakie podjąć kroki, by ewentualne przeprowadzenie zmiany drogi pakietów i podsłuch nie miały bezpośredniego wpływu na bezpieczeństwo sieci komputerowej.

2. Jak nie dopuścić do możliwości przeprowadzenia opisywanego ataku.

Jeśli chodzi o pierwsze zagadnienie, to należy zastosować wszelkie metody zapobiegania atakom typu sniffing. Skuteczną metodą jest szyfrowanie przesyłanych informacji. Przykładem dobrego rozwiązania jest system Secure Shell czy też pakiet Pretty Good Privacy.

Secure Shell (ssh) jest szczególnie wygodny z tego względu, iż z punktu widzenia użytkownika realizowanie takich czynności, jak zdalna praca czy też transfer plików odbywa się dokładnie w ten sam sposób jak w przypadku tradycyjnych narzędzi, takich jak rsh, ftp czy rlogin. SSH zabezpiecza również przed przejęciem przez intruza sesji TCP .

W dalszej części przedstawione zostaną metody mające na celu uniemożliwienie przeprowadzenia opisywanego ataku.

6.1. Statyczne odwzorowanie adresów IP na adresy sprzętowe

Pierwszym nasuwającym się pomysłem jest zrezygnowanie z protokołu ARP. Rozwiązanie to jest możliwe w praktyce, choć wymaga dodatkowej pracy administratora sieci zarówno w okresie początkowym, jak i w czasie eksploatacji i rozbudowy sieci.

Zrezygnowanie ze stosowania protokołu ARP wymaga użycia statycznej tablicy ARP, inicjowanej podczas startu systemu i aktualizowanej w miarę rozbudowy sieci. Tablica ta powinna zawierać odwzorowanie adresów IP na adresy sprzętowe wszystkich urządzeń pracujących w sieci. Oczywiście na każdym komputerze powinna znajdować się identyczna tablica.

Istotną wadą tego rozwiązania jest konieczność aktualizacji tablicy ARP wszystkich komputerów w sieci w przypadku zmiany interfejsu sieciowego lub rozbudowy sieci o nowe urządzenia.

6.2. Analiza pakietów ARP

Inna metoda polega na analizie pakietów protokołu ARP w celu wykrycia podejrzanych zmian. Zmiany adresów sprzętowych występują w rzeczywistej sieci komputerowej bardzo rzadko, więc nie trudno zrealizować oprogramowanie ostrzegające administratora sieci o zmianach odwzorowania adresów IP na adresy sprzętowe. Jednym z darmowo dostępnych narzędzi tego typu jest program arpwatch dostępny pod następującym adresem: ftp://ftp.ee.lbl.gov/arpwatch-*.tar.Z .

7. Podsumowanie

Niniejsze opracowanie miało na celu ukazanie luk bezpieczeństwa w protokole ARP. Opisywana metoda ataku stanowić może punkt wyjściowy dla prowadzenia dalszej działalności intruza. Mając możliwość podsłuchu przesyłanych w sieci pakietów, jak również ich modyfikacji, intruz jest w stanie sparaliżować pracę sieci komputerowej (denial of service), wykraść czy też usunąć pliki przechowywane na dyskach.

Należy jednocześnie zwrócić uwagę, iż ze stosowaniem urządzeń typu bridge oraz switch wiąże się również zagrożenie wynikające z realizowanego przez te urządzenia protokołu budowy drzewa rozpinającego. Protokół ten podobnie jak protokół ARP nie posiada żadnych mechanizmów ochronnych. Istnieje zatem możliwość celowego odłączenia całego segmentu sieci odpowiednio preparując i wysyłając pakiety protokołu drzewa rozpinającego.

Obecność w sieci komputerów pracujących pod kontrolą systemów DOS, Windows 3.X czy też Windows 95 jest poważnym zagrożeniem bezpieczeństwa całej sieci. W systemach tych każdy użytkownik ma możliwość wysłania pakietów sieciowych z zafałszowanymi polami, włączając w to również pola adresów sprzętowych. Należy mieć ten fakt na uwadze podczas włączania do sieci uznawanej za bezpieczną nowych komputerów. Jak wynika z niniejszego artykułu, nawet separacja stacji za pomocą switcha nie jest rozwiązaniem pewnym.

LITERATURA

[1] Stevens W. R.: „TCP/IP Illustrated Volume 1 The Protocols", Addison-Wesley, 1994.

[2] Stevens W. R.: „TCP/IP Illustrated Volume 2 The Implementation", Addison-Wesley, 1995.

[3] Tannenbaum A. S.: „Computer Networks 3rd Edition", Prentice Hall, 1996.

[4] Plummer D.C.: „An Ethernet Address Resolution Protocol", RFC 826, 1982.

Recenzent: Dr inż. Mirosław Skrzewski

Wpłynęło do Redakcji 12 grudnia 1997 r.

Abstract

Address Resolution Protocol is a fundamental part of the TCP/IP protocol suite. It provides mapping between network layer logical address and data link layer hardware address. The idea of the ARP is shown on fig. 2. Before sending the IP datagram, host 10.0.0.2 broadcasts an ARP request packet. This packet is being received by all hosts in the physical Ethernet segment, but only one of them, the one with IP address 10.0.0.1 should send the ARP reply message. To reduce unnecessary broadcast traffic, each host maintains ARP cache.

Though simple, efficient and transparent to the network administrator (requires no manual configuration), ARP has absolutely no security mechanisms. By spoofing ARP packets a potential intruder is able to change the path of the IP packets. This technique of active packet path redirection, as opposed to the traditional passive sniffing, allows the intruder to sniff the IP packets even in the presence of the MAC level filtering devices such as bridges or LAN switches.

In the example configuration shown on fig. 1 an intruder equipped with the passive sniffing software is able to perform the monitoring of multicast and broadcast packets transmitted between hosts A and B. This kind of packets usually carry no crucial data such as network passwords. The intruder can however modify the path of IP packets by sending spoofed ARP reply packets to hosts A and B. This attack method takes advantage of the TCP/IP implementation feature that host accepts ARP reply packets even if it didn't ever send the corresponding ARP request. This behaviour is quite common in the popular operating systems like MS Windows NT, Linux or SunOS. Using this technique the intruder is able to examine the content of all IP packets, modify and send them to the true destination system (fig 4).