논문 2008-45TC-1-3

BcN(Broadband Convergence Network) 환경에서의 중요정보에 대한 도청방지 메카니즘

(The core information protection mechanism in the BcN(Broadband Convergence Network))

오 석 환*, 이 재 용**, 김 병 철**

(Sek Hoan OH, Jae Yong Lee, and Byung Chul Kim)

요 약

인터넷 접속기술로서 IP over Ethernet 기술이 널리 상용화되어 적용되고 있는데 이 기술은 IP 주소를 MAC 주소로 변환하기 위한 주소번역 프로토콜로서 ARP(Address Resolution Protocol)를 사용하고 있다. 최근들어 이러한 ARP에 대한 보안 공격은 IP 주소와 이와 대응하는 MAC 주소를 의도적으로 변경하는 공격으로서, 이를 수행하기 위해 "snoopspy"등과 같은 다양한 툴을 사용한다. ARP 공격을 수행함으로써 원래 의도한 목적지와는 다른 MAC 주소로 패킷을 보내어, 공격자가 내용을 도청하거나, 내용을 변경하거나, 연결을 가로채기 할 수 있다. ARP 공격은 데이터링크 계층에서 수행되므로 Secure Shell(SSH) 또는 Secure Sockets Layer(SSL)와 같은 방법에 의해 방어할 수 없다. 따라서 이 논문에서는 ARP 공격을 방향성에 따라 하향공격인 ARP spoofing 공격과 상향공격인 ARP redirection 공격으로 각각 분류하고, IP주소를 획득시 얻는 DHCP 정보를 이용하여 대처하는 새로운 보안 기법을 제안하였다. 즉, ARP spoofing 공격에 대해서는 "DHCP snoop 기법" 또는 "DHCP sniffing/inspection 기법"을 제안하였고, ARP redirection 공격에 대해서는 "static binding" 기법을 제시하였다. 이 논문에서 제안한 ARP 공격은 BcN을 비롯한 차세대 인터넷 접속망의 보안성을 강화하는데 널리 사용될 수 있을 것이다.

Abstract

IP over Ethernet technology widely used as Internet access uses the ARP(Address Resolution Protocol) that translates an ip address to the corresponding MAC address. recently, there are ARP security attacks that intentionally modify the IP address and its corresponding MAC address, utilizing various tools like "snoopspy". Since ARP attacks can redirect packets to different MAC address other than destination, attackers can eavesdrop packets, change their contents, or hijack the connection. Because the ARP attack is performed at data link layer, it can not be protected by security mechanisms such as Secure Shell(SSH) or Secure Sockets Layer(SSL). Thus, in this paper, we classify the ARP attack into downstream ARP spoofing attack and upstream ARP redirection attack, and propose a new security mechanism using DHCP information for acquisition of IP address. We propose a "DHCP snoop mechanism" or "DHCP sniffing/inspection mechanism" for ARP spoofing attack, and a "static binding mechanism" for ARP redirection attack. The proposed security mechanisms for ARP attacks can be widely used to reinforce the security of the next generation internet access networks including BcN.

Keywords: ARP attack, eavesdrop, session hijecking, network security

* 정회원, (주)KT
(KT Corp.)
** 종신회원, 충남대학교 전기정보통신공학부
(Division of Electrical and Computer Engineering, Chungnam National University)
※ "본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업[2007-S001-01, 2007-F-038-01]과 한국과학재단(No. R01-2006-000-10154-0) 사업의 일환으로 수행하였음"
접수일자: 2007년11월14일, 수정완료일: 2008년1월15일

Ⅰ. 서 론

인터넷의 범용성과 접근 용이성으로 인해 정보 공유, 검색 및 자료 교환 등의 편의성이 증대되고 있으며, 또한 인터넷 상에서의 흘러 다니는 수많은 정보는 일반 범용적인 정보에서부터 전자상거래, 개인 메일, ID/Password 등 security가 중요한 정보들까지 그 종류가

다양하여, 그 보안 대처방안에 대해서도 많은 연구가 진행 중이다.

그 중 broadcasting되는 ARP의 특성을 이용하여, 동일 링크 구간에서 사용되는 타 사용자 단말의 MAC 주소를 알아내고, 이를 이용하여 자신이 상대방 단말인 것처럼 spoofing하거나 redirection한 후 원래의 목적지로 넘겨주는 방식으로 상대방 정보를 교묘히 알아내는 일명 가로채기 기능을 할 수 있는 공개 해킹 프로그램이 사이버 상에서 돌아다니고 있다. 이는 일반 개인 자료의 누출뿐 아니라 특히 전자상거래 시 ID/Password 노출의 가능성도 있어 인터넷 사용자에게 큰 피해를 줄 수 있는 보안상의 취약점이다[1~3].

실제로 해킹프로그램을 이용한 MSN 메신저 도청 프로그램 등장이라는 뉴스가 2005년에 소개된 적이 있으며, 네트워크 트래픽 및 장애 분석 시 이러한 원인 때문에 생긴 장애 확률이 점차 증가되고 있는 실정이다[4~5].

본 논문에서는 이러한 ARP 공격을 해결하기 위해 현재 ISP(Internet Service Provider)망에서 일어나는 하향 방향의 ARP spoofing 공격에 대해서는 DHCP snoop 기능 또는 sniffing과 ACL 기능을 이용하고, 기준 DB로서 DHCP 과정에서 얻어진 정보를 이용하는 방법을 제시하였다. 또한 상향 공격에 대해서는 일명 static binding 기법을 이용하여 ARP 공격에 대한 방어를 완벽히 할 수 있는 기법을 제시하였다.

향후 BcN망은 단말 인증 및 소프트웨어 자동 업그레이드 등을 위하여 고정 IP 할당방식에서 유동 IP방식인 DHCP 할당방식으로 점차적으로 전환되고 있는 실정이며 이는 가입자 단말이 네트워크에 접속 시 IP할당을 요청하게 되고, 이때 인증서버와 연동하여 정당한 가입자이면 인증 성공과 동시에 DHCP 서버로부터 IP를 할당하고, 또한 DHCP 정보에 단말의 소프트웨어 최신버전, TFTP 주소정보, 접속서버 정보 등 다양한 정보를 함께 보내줄 수 있어 이를 통해 단말 인증, 자동 업그레이드등의 응용에 사용될 수 있다. 또한 BcN에서는 장애 및 운용 관리를 위한 댁내 망 및 가입자 망의 형상관리, end-to-end QoS 제공을 위하여 DHCP option 82를 이용하는 방안이 검토 중이며, 이러한 DHCP를 이용한 방안은 ARP 공격에 대한 대처 방안 뿐 아니라 향후 BcN망에서의 다양한 응용에도 사용될 수 있다.

본 논문은 먼저 근래에 문제점으로 크게 대두되고 있는 ARP 공격의 현 상황 및 인터넷에서 유포중인 해킹툴인 snoop-spy 등의 ARP 공격 프로그램[6]의 특징 및 동작을 Ⅱ장에서 소개하였으며, Ⅲ장에서는 이를 방지하기 위한 대안으로 현재 고려중인 기술인 S-ARP기술[8]과 네트워크 장비기술인 공유 VLAN[9], proxy ARP, gratuitous ARP 등의 공격 차단 기능과 문제점에 대해 기술하였다. Ⅳ장에서는 새로운 ARP 공격 대처방안인 DHCP snoop binding, DHCP sniffing과 DHCP static binding 기법을 제안하였다. 특히 ARP attack에 대해서 하향 트래픽 공격(ARP spoofing attack)에 대한 탐지 및 차단 방법과 상향 트래픽 공격(ARP redirection attack)에 대한 탐지 및 차단 방법을 별도로 고려하였고 DOS(Denial Of Service)형 ARP 공격[13]에 대한 방어수단에 대해서도 제시하였다. Ⅴ장에서는 제시한 ARP 공격 대응방안을 구현하여 실제 실험한 결과 내용을 설명하였고, 마지막으로 Ⅵ장에서는 현 네트워크 장비의 하드웨어 성능으로 인해 새로운 기술을 적용하지 못할 경우 및 고정 IP 가입자에 대한 향후 연구내용을 제시하고 결론을 맺는다.

Ⅱ. ARP Attack

1. ARP 공격이란?

ARP 공격은 스위치로의 직접적인 공격이 아닌 트래픽의 흐름을 변경하는 트래픽 흐름 변경 공격이라고 할 수 있다. 그림 1은 상향 트래픽에 대한 ARP redirection 공격으로서 공격자는 위조된 ARP reply 메세지를 보내는 방법을 이용한다. 공격자가 도청 가능한 이유는 PC를 promiscuous mode로 동작하게 공격 프로그램에서 설정하기 때문이다[1].

이를 위해 공격자는 '내 MAC 주소가 라우터(게이트웨이)의 MAC 주소이다.'라는 위조된 ARP reply를 broadcast로 네트워크에 주기적으로 보내어, 스위칭 네트워크상의 다른 모든 호스트들이 공격자 호스트를 라우터로 믿게끔 한다. 따라서 외부 네트워크와의 모든 트래픽은 공격자 호스트를 통하여 지나가게 되고 공격

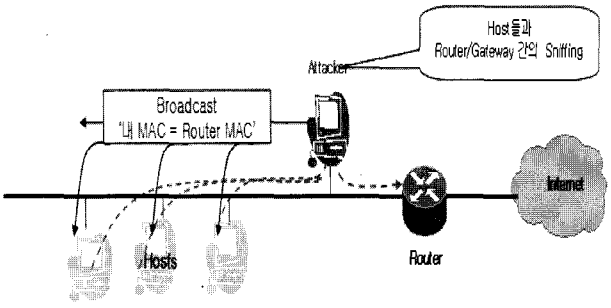


그림 1. 상향트래픽 공격인 ARP redirection 공격
Fig. 1. ARP redirection attack for Uplink traffic.

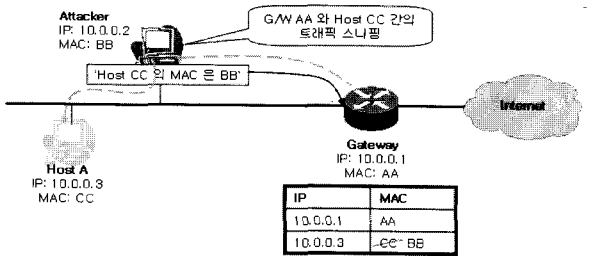


그림 2. 하향 트래픽 공격인 ARP spoofing 공격
Fig. 2. ARP Spoofing attack for downlink traffic.

자는 패킷 capture 프로그램을 통해서 필요한 정보 도청이 가능하다. 이때 공격 호스트는 IP forwarding 기능을 설정하여, 공격 호스트로 오는 모든 트래픽을 원래의 호스트 또는 게이트웨이로 전달해 주어야한다.

그림 2는 하향 트래픽에 대한 ARP spoofing 공격으로서 공격자는 자신의 MAC 주소를 sniffing하고자 하는 호스트의 MAC 주소로 위장하는 ARP reply 패킷('sniffing 하려고 하는 호스트의 MAC 주소는 내(공격자) MAC 주소다'라는 패킷)을 호스트와 라우터에 보낸다. 이러한 ARP reply를 받은 호스트와 라우터는 자신의 ARP cache 테이블을 업데이트 하게 되고, 호스트간의 연결이 일어날 때 공격자 호스트의 MAC 주소를 사용하게 된다.[2~3]

2. ARP 공격프로그램(Snoopspy 등)

현재 인터넷상에서 많은 ARP 공격이 돌아다니고 있으며, 실제로 이를 통해 개인정보유출 및 인터넷 이용장애 등 많은 문제점이 발생되고 있다.

그 중 그림 3은 일반적으로 쉽게 구할 수 있는 ARP 공격 중 snoopspy의 공격을 캡처한 것으로서, 이 프로그램은 공격하고 싶은 host (동일 subnet)를 지정하여,

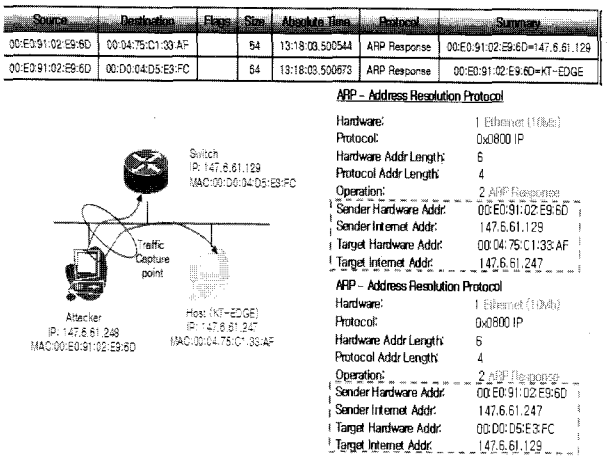


그림 3. 패킷 분석기에 의한 ARP 공격분석
Fig. 3. ARP attack analysis by packet analyzer.

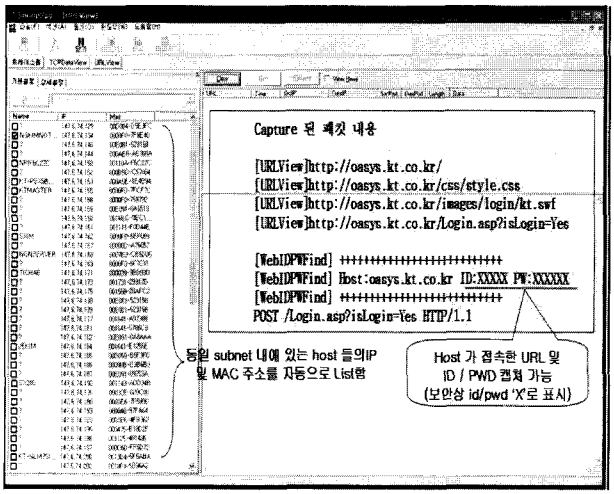


그림 4. ARP 공격프로그램에 의한 실행 예
Fig. 4. The execution example by ARP attack program.

그 host 에서 발생되는 모든 network data를 capturing 하는 프로그램이다. 방법은 ARP reply 메시지를 변경하여, 그림 3과 같은 두 개의 ARP reply 메시지를 발생하는 것인데, 그 이후 host 에서 발생하는 모든 트래픽은 공격자를 통해 전달된다. 현재 sniffing attack을 하기 위해선 사이트에서 무료로 다운로드 받을 수 있는 snoopspy 같은 소프트웨어를 설치하는 방법 외에도 간단한 unix 명령어를 이용하여 file 몇 개만을 실행하면 간단한 명령어만으로도 충분히 가능하며, 특히 FTP, HTTP, POP 등 많은 프로토콜들은 사용될 때 전혀 암호화 되지 않고 있으므로 그 심각성이 어느 때보다도 높다고 할 수 있겠다[6].

snoopspy 프로그램을 설치하면 그림 4와 같이 나타나는데, 여기서 찾고자 하는 공격목표의 게이트웨이와 subnet을 정해주고 실행을 하면 해당 subnet에 속하는 host 중 현재 동작중인 host의 ARP request에 대한 응답으로 IP와 MAC 정보를 포함한 정보가 나타나게 되고 박스 체크를 한 후 열기를 하면 해당 host 정보를 일명 가로채기 방식으로 얻을 수 있다[7~8].

그림 4는 snoopspy software를 실제적으로 설치하여 동작시켰을 때 볼 수 있는 화면으로서 왼쪽부분은 현재 동일 subnet에 속해있는 장비의 IP주소와 MAC을 보여주며, 오른쪽은 공격당하는 장비에서 통신하고 있는 내용이 capture된 부분이다. 그림의 오른쪽 부분에서 확인할 수 있는 것과 같이 host가 통신하는 ID와 password도 쉽게 알아낼 수 있다.

3. 네트워크상에서의 실제 ARP 공격의 예

ARP 공격에 의한 실제 공격 발생 상황을 현재 운용

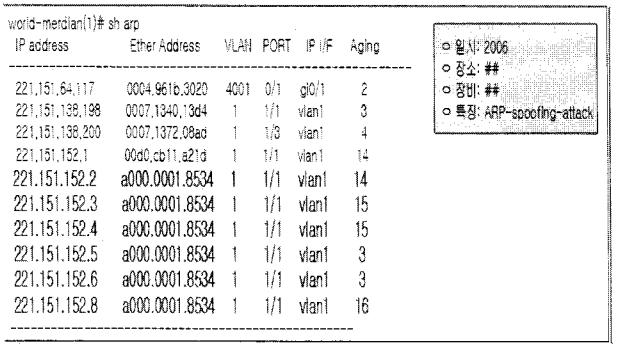


그림 5. 인터넷상에서의 ARP 공격에 의한 실제 공격
Fig. 5. Real ARP attacks on the Internet.

중인 네트워크 장비에서 분석한 자료는 그림 5와 같으며 굵은 글씨로 표시된 바와 같이 다른 IP에 동일한 MAC 정보가 매핑 되어있는 ARP spoofing 공격임을 알 수 있다. 이로 인해 가입자 정보 누출 및 장애 원인이 될 수 있으며, 최근 그 발생 빈도가 점차 증가하고 있는 상황이다.

Ⅲ. 기존 기술을 이용한 ARP 공격 차단 방안

본 장에서는 ARP 공격에 대한 차단방안으로 S-ARP, 공유 VLAN 등을 이용한 기존 제안된 기법을 분석하고 결과 및 문제점 등을 도출한다.

1. S-ARP(Secure ARP)

ARP 프로토콜은 불특정 host의 IP에 해당하는 MAC을 찾기 위한 프로토콜이므로 자체적인 보안기법은 적용되지 않는 실정이며, 또한 Secure Socket Shell(SSH) 또는 Secure Sockets Layer(SSL)등 상위 계층에서의 보안 기술을 이용하여 공격을 방어할 수 없는 실정이다.

따라서 대응 방안 중 인증된 한 쌍의 키를 사용하는 secure ARP[10]를 이용하는 방안이 제안되었다. 각 host들은 LAN상에서 지정된 CA(Certifcation Authority)와 같이 동작하는 local trusted party에 의해 증명된 공개키/비밀키 쌍을 가지고 있으며 이를 통해 전달되어온 ARP 패킷이 정당한 권리자의 것인지 여부를 확인함으로써 ARP 공격에 방어를 할 수 있는 방법이다. 이 방안의 특징은 다음과 같다.

- 어떠한 계층에서의 공격에 대해서도 방어가 가능한 가장 확실한 수단이다.
- 이러한 키 값에 대한 정보를 위하여 추가적인 header가 필요하다.
- S-ARP 메시지는 S-ARP 프로토콜을 채용하지 않은 호스트에 의해 처리될 수 있지만 S-ARP 프로토콜을 채용한 host는 non-authenticated 메시지(기존 ARP 프로토콜)를 처리할 수 없다.
  interoperability 문제가 발생한다.

S-ARP 방안은 키 값과 인증서를 이용하여 사용자 인증뿐 아니라 메시지 인증을 동시에 할 수 있는 기법으로서 MAC 뿐 아니라 상위 layer의 프로토콜에 공통적으로 적용될 수 있어서 범용성과 확장성이 있다는 장점이 있지만, 동일 LAN 내부에 키 값을 검증해주는 AKD(Authentication Key Distributer)를 운용하여야 한다는 점과 모든 LAN의 host에서 동일하게 S-MAC을 운용하여야만 공격에 방어를 할 수 있다는 단점이 있다.

2. 공유 VLAN 및 Proxy ARP 기술을 조합한 기법

가. 현재의 접속망 구조 및 발전 방향

현재 인터넷망의 가입자 네트워크는 모두가 broadcast domain으로 구성되어 있기 때문에 broadcast 트래픽이 동일 subnet에 속한 모든 가입자에게 전달되는 구조이다. 즉, 현재 일반 ISP의 접속망은 ARP를 이용한 해킹을 시도할 경우, 방지할 수 있는 능력이 없는 구조로서 해킹 등을 원천적으로 차단할 수 있게 네트워크 구조를 변경/설계하여야 보안이 강화된 망 기능 변경이 이루어진다.

실제로 현재의 네트워크에서 ARP 트래픽은 그림 6과 같이 동일 subnet내의 모든 호스트로 전달되며 이로

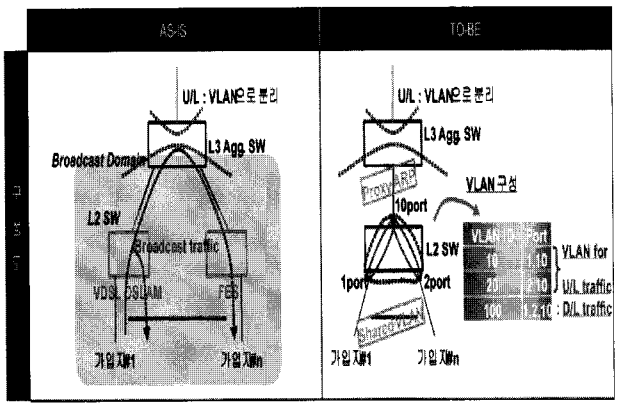


그림 6. 현재의 접속망 구조 및 개선 구조
Fig. 6. Current structure of access network structure and its evolution.

인해 정보 sniffing이 용이한 구조이고, 동일 L3내에 수용된 가입자의 정보가 평문으로 전송될 때 ARP 공격으로 인해 중요 정보 누출이 용이한 네트워크 구조이다. 따라서 ISP들은 접속망 구조를 그림 6의 오른쪽 그림에서와 같은 TO-BE 구조로 진화하려고 노력 중이다. 이는 가입자의 broadcast 트래픽을 물리적으로는 동일하지만 논리적으로 분리할 수 있게 한 구조로서 L2 스위치의 공유 VLAN 정책 등이 적용 되어 있다.

나. 시험 시나리오 및 결과

P2P 통신의 불가능이라는 문제점을 해결하기 위해서는 공유 VLAN 이외에 게이트웨이에 ARP proxy기능을 지원하여야 한다. 그림 7은 proxy-arp를 추가 적용한 경우인데 이는 공격자와 host가 다른 L2 스위치에 존재할 때는 ARP 공격을 방지할 수 있는 구조이지만 동일한 L2 스위치에 존재할 때는 일명 pingpong 현상으로 인해 공격차단 뿐 아니라 정상적인 인터넷 사용도 할 수 없다는 문제점이 발생한다[9]. 즉 동일 L2 스위치에 공격자와 host가 존재할 때 L3 스위치의 ARP proxy 기능에 의해 공격자는 10.1.1.10의 MAC 주소를 L3 스위치의 MAC인 AA로 알게 되어 아래에서 보듯이 일명 pingpong 현상이 발생한다. 동작 순서는 다음과 같다.

하향 트래픽의 경우 L3 스위치의 ARP table을 본 후 MAC이 CC인 공격자로 보낸다.

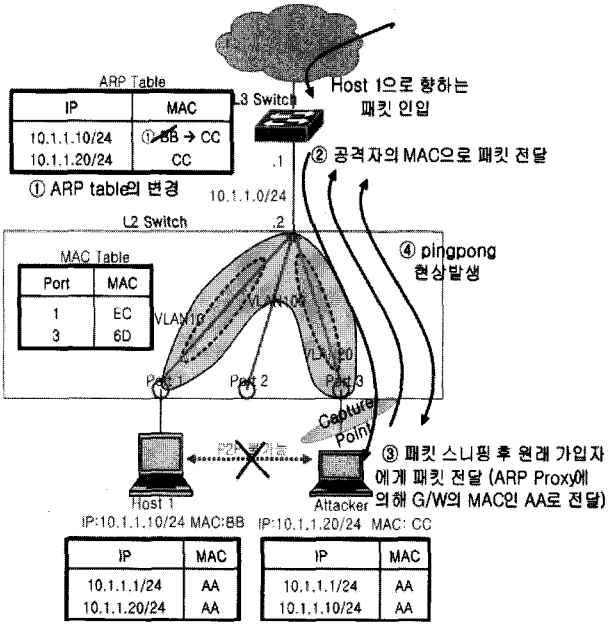


그림 7. ARP 프록시를 이용한 중첩 VLAN
Fig. 7. Shared VLAN with ARP Proxy.

- 공격자는 패킷을 sniffing한 후 정상적인 수신자인 Host1이 패킷을 받을 수 있도록 목적지 IP와 MAC(10.1.1.10, BB)으로 수정한 뒤 L3 스위치로 패킷을 보내게 된다.
- L3 스위치는 목적지 IP에 대응하는 MAC을 찾기 위해 자신의 ARP table을 검색한 후 해당하는 MAC (CC: 공격자 MAC)으로 변경하여 패킷을 보낸다.
- L2 스위치는 자신의 MAC table에서 목적지 MAC에 해당하는 인터페이스로 패킷을 보내며 공격자가 해당 패킷을 받게 된다.
- 공격자는 다시 L3 스위치로 패킷을 보낸다. (일명 ping-pong 현상)

따라서 정상적인 가입자(Host1)는 인터넷을 사용할 수 없게 되어 민원발생의 소지가 있어서 적용할 수 없는 구조이다.

그림 8은 동일 L2 스위치에 가입자와 공격자가 존재하는 ARP Proxy를 가지는 공유 VLAN 기능 시험 결과를 패킷 분석기로 캡처한 것으로서 결과적으로 L3 스위치의 게이트웨이 MAC 주소를 변경 방지함에 의해서 ARP redirection에 의한 host 정보의 유출은 방지할 수 있지만, L3 스위치에 ARP proxy 기능을 enable 시키면 공격을 당한 host가 인터넷을 사용할 수 없는 현상이

Source	Destination	Class	Size	Absolute Time	Protocol	Summary
00:E0:91:02:E9:6D	00:D0:F0:65:D9:EC		64	11:17:07.668224	ARP Response	00:E0:91:02:E9:6D=10.1.1.1
00:E0:91:02:E9:6D	00:D0:CB:0A:A4:67		64	11:17:07.668344	ARP Response	00:E0:91:02:E9:6D=10.1.1.10
00:E0:91:02:E9:6D	00:D0:F0:65:D9:EC		64	11:17:08.669687	ARP Response	00:E0:91:02:E9:6D=10.1.1.1
00:E0:91:02:E9:6D	00:D0:CB:0A:A4:67		64	11:17:08.669779	ARP Response	00:E0:91:02:E9:6D=10.1.1.10

ARP Proxy설정한 경우 Attacker으로 부터의 packet capture

그림 8. 캡처된 패킷 분석
Fig. 8. Analysis of captured packet.

표 1. 시나리오에 따른 시험결과
Table 1. Test results under various scenarios.

	동일 L2 S/W에 수용 시	다른 L2S/W에 수용 시
Shared VLAN Without ARP Proxy	P2P (X) 인터넷 (o) Sniffing (X)	P2P (o) 인터넷 (o) Sniffing (o)
Shared VLAN With ARP Proxy	P2P (X) 인터넷 (X) Sniffing (X)	P2P (o) 인터넷 (o) Sniffing (o)
Shared VLAN With ARP Proxy (Port Isolation 적용)	P2P (X) 인터넷 (X) Sniffing (X)	P2P (o) 인터넷 (o) Sniffing (X)

발생하게 된다.

표 1은 기존 기술을 이용하여 시험한 종합 결과로서 공유 VLAN 및 ARP Proxy 기능을 적용 시에 공격자와 호스트가 별도의 L2 스위치에 존재할 때에는 ARP 공격에 대응할 수 있으나, 동일 L2 스위치에 연결되어 있을 때는 sniffing이 불가능 하게 되는 반면, 인터넷과 P2P 연결은 되지 않는다는 문제점이 발생함을 보여준다.

3. Gratuitous ARP 기법

Gratuitous ARP 기술은 현재 일부 장비 업체에서 개발하여 적용중인 것으로 어떤 host가 자기 자신의 IP 주소에 대해 ARP request를 송신하여, 여기에 대한 답이 오면 자기 자신과 같은 IP 주소를 누군가 쓰고 있는 것이므로 IP 주소의 중복사용을 막는 기능으로 사용하는 것이다.

그림 9와 같이 일부 L3 스위치에서는 일명 ARP-patrol 기능(gratuitous ARP)을 L3 스위치에 설정함으로써, L3 스위치의 MAC을 주기적으로 보낸다. Interval과 count(송신할 ARP 패킷의 숫자)를 지정할 수 있으며, Windows 계열의 PC가 유동 IP를 할당 받고 난 후, 해당 IP의 사용유무를 확인하기 위한 gratuitous ARP 패킷을 발생한다.

문제는 gratuitous ARP 기능을 사용하여도 snoopspy와 같은 프로그램의 경우 1초에 약 2개의 위조된 ARP response를 보내므로, MAC 테이블이 위조된 MAC으로 다시 변경된다는 한계가 있다. 그러므로 gratuitous ARP에 의해 sniffing을 방지하는 것이 불가능하다. 즉, gratuitous ARP 동작 시 게이트웨이에서 자신의 MAC을 주기적으로 전송하도록 주기 및 횟수를 정하여 가입자에게 발송하면 host에서는 공격자로부터의 공격으로부터 자신의 ARP table이 변경되더라도 다시 갱신하여 정상적인 테이블로 원복 할 수 있지만 만약 공격자가 게이트웨이보다 더 빠른 주기로 공격 시

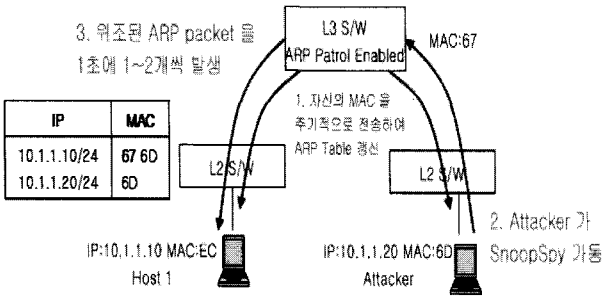


그림 9. Gratuitous ARP 동작
Fig. 9. The operation of Gratuitous ARP.

완벽하게 ARP redirection 공격을 방어할 수 없다는 문제점이 발생한다.

Ⅳ. DHCP snoop 기능과 Static Binding 기술을 이용한 ARP 공격 방지 기법

ARP 공격에 대한 대처 방안으로 제시된 공유 VLAN, proxy ARP, port isolation 등의 다양한 기술 등을 사용하여도 완벽한 ARP 공격 차단이 불가능함에 따라 별도의 방안이 필요하다. 이 또한 상향공격인 ARP redirection 공격과 하향공격인 ARP spoofing 공격을 구별하여 적용함으로써 다양한 ARP 공격에 대처하여야 한다. 또한 DOS형 ARP 공격에 대해서는 최대 ARP 트래픽 허용치인 threshold 값을 정하고, 이보다 높으면 폐기시키는 DOS 방어기법도 고려되어야 한다.

1. ARP Spoofing 공격에 대한 방어기법

가. ARP payload 내의 정보 추출

ARP spoofing 공격을 차단하기 위해서는 전달되는 ARP 패킷의 payload내 MAC의 진위여부를 가려서 틀리면 MAC 테이블에 등록되는 것을 불허하여 실제 가입자 트래픽이 악의의 공격자로 전달되는 것을 방지할 필요가 있다. 이를 위해서는 그림 10과 같이 ARP payload내의 source MAC과 source IP를 추출하여 L2 스위치에 저장된 DHCP 관련 DB 값과 비교하는 기법이 필요하다. 따라서 전송되는 ARP 패킷의 payload 부분에 포함된 source MAC과 source IP을 알아내기 위해 패킷을 decapsulation하는 기능이 필요하다.[10]

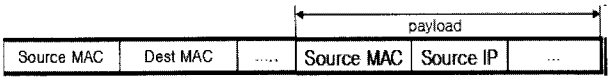


그림 10. DHCP 정보와 비교를 위한 ARP 패킷의 페이로드
Fig. 10. ARP packet payload for comparing with DHCP information.

나. DHCP snoop binding 기법

하향 공격인 ARP spoofing 공격에 대처하기 위해서는 DHCP snoop이라는 기술을 이용하여 입력되는 ARP 정보에 대하여 옳은 정보인가를 비교하고, 공격에 대해서 차단하는 기법이 필요한데, 동작 과정은 그림 11과 같다.

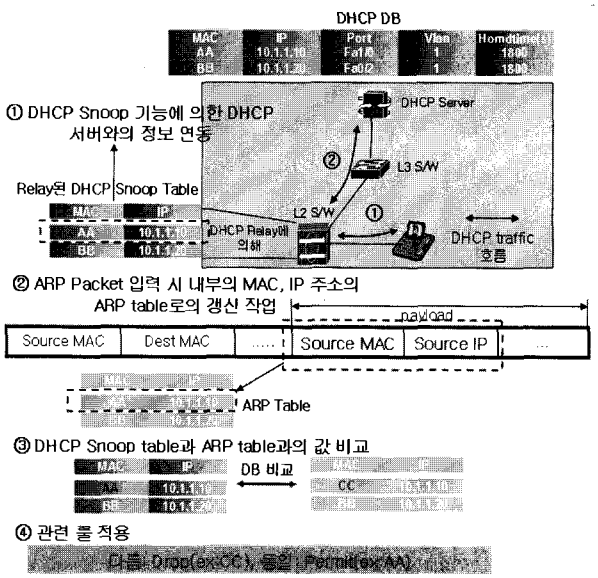


그림 11. DHCP snoop 바인딩 기법에 의한 동작절차
Fig. 11. Procedure of DHCP snoop binding scheme.

- ARP 테이블과의 비교를 위한 기준 DB 구성을 위해 각 가입자단의 L2 스위치에 DHCP snoop 기능을 적용하여 DHCP 할당과정에서 얻은 MAC과 IP를 DHCP snoop binding table에 저장하는 과정
- ARP 패킷이 스위치로 입력 시 내부의 MAC과 IP를 알기 위해 decapsulation하여 ARP table을 갱신하는 과정
- DHCP snoop binding table과 ARP table을 비교하는 과정
- 비교하여 같으면 ARP 패킷을 내부 네트워크로 통과시키고, 다르면 폐기시키는 ACL(Access Control List) 정책의 적용 과정

DHCP 서버에 등록된 정보는 가입자가 제일 먼저 인터넷에 접속하기 전 IP 할당과정에서 얻어진 정보이므로 어떤 정보보다 정확하고, 믿을 수 있는 정보라 할 수 있다.

다. DHCP Snoop 기능 적용시 문제점 및 해결방안

DHCP 서버 정보를 이용하기 위해서는 각각의 스위치에 DHCP relay 기능을 동작시켜야 하는데, DHCP discover, request 시에는 트래픽이 broadcast 되는 특성상 해당 단말을 수용하는 L2 스위치뿐 아니라 상위의 L3 스위치 및 다른 L2 스위치로 전파된다는 특징이 있다.

즉, 단말에서 보내진 DHCP packet이 그림 12와 같이 L2 자체 내에 설정된 DHCP relay를 통해 DHCP 서버

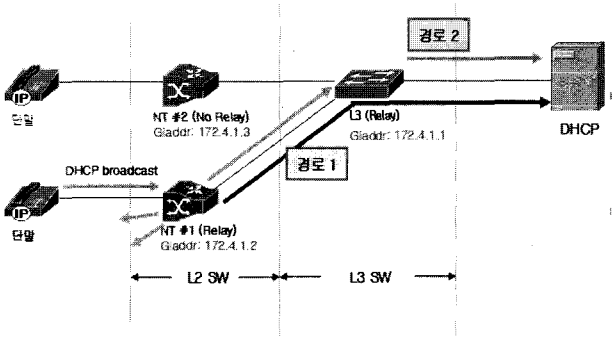


그림 12. 2개의 L2 스위치에서의 DHCP 릴레이 시험
Fig. 12. DHCP Relay test with two L2 switches.

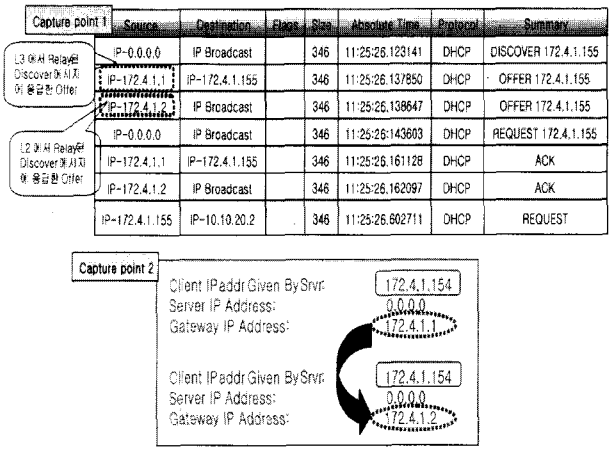


그림 13. 두개의 L2 스위치에서의 DHCP 릴레이 시험결과
Fig. 13. Test result of DHCP relay with two L2 switches.

까지 가는 "경로 1"과 L2에서 broadcast 된 후 L3까지 가서 L3에서 릴레이되는 "경로 2"의 두 가지의 경로가 존재한다. 따라서 DHCP server에 동일 DHCP 요구 및 IP 할당이 별도로 중복되어 발생되며 만약 L3 하단의 L2 스위치가 여러 개라면 해당 L2 스위치 개수만큼 DHCP 패킷의 중복 등록이 발생될 수 있어, DHCP 서버 부하 증가 및 네트워크 대역폭의 과다 이용 등의 문제 등이 발생될 수 있다.

그림 13은 DHCP 서버 앞단에서 실제로 관련 패킷을 캡처하여 분석한 것으로서 어느 스위치에서 릴레이된 메시지인가에 관계없이 가장 나중에 DHCP 서버로 유입된 스위치에 대한 정보가 저장된다. 따라서 스위치의 수 및 DHCP 트래픽이 증가할수록 DHCP 서버의 부하 증가 및 네트워크 대역폭 소모의 단점이 발생된다는 문제가 발생한다.[11~12]

이에 대한 해결방안으로 L2 릴레이와 L3 릴레이가 혼재된 상황에서 스위치를 DHCP 릴레이로 사용하려면 릴레이되는 unicast packet 이외의 broadcast packet을 in/out 방향 모두에서 filtering하여야 한다. 결론적으로

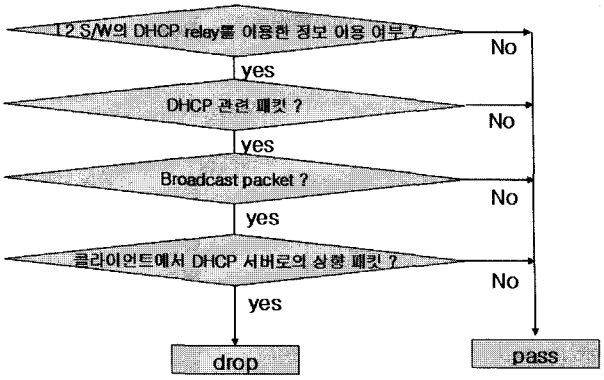


그림 14. DHCP egress filtering 적용 순서도
Fig. 14. The flow diagram for DHCP egress filtering.

DHCP 트래픽에 대한 egress filtering기법은 ingress filtering보다 필터링 룰이 적용되는 스위치 및 포트의 갯수를 줄일 수 있고, 이로 인해 장애의 확률도 줄일 수 있다는 장점이 있다.

Egress filtering의 적용 순서도는 그림 14와 같으며 먼저 스위치에서의 DHCP relay 기능을 이용한 snoop 기법이 적용되었는가를 판단 후 DHCP 관련 패킷이 입력되면, 그 중 unicast인가 broadcast인가를 판단하고 broadcast 패킷이면 클라이언트에서 DHCP 서버로의 패킷 여부를 다시 분석 후 상향 방향이면 egress port에서 폐기하고, 하나의 조건이라도 일치하지 않으면 통과시켜서, DHCP로의 이중 등록 방지 및 서버 부하 문제를 해결할 수 있다.

라. DHCP sniffing 및 inspection을 이용하는 방법

DHCP relay 기능을 이용하는 DHCP snoop binding 기법은 스위치에서 별도의 DHCP에 관한 relay 기능을 적용함으로써 부하증가가 있을 수 있으며, broadcast되는 DHCP 패킷이 타 스위치로 전파되지 않게 하기 위해 복잡한 ingress filtering 또는 egress filtering 기법을 적용하여야 한다.

이 문제를 해결하기 위해 스위치에서 DHCP 트래픽에 대해서 sniffing하여 DHCP snoop binding table과 동일한 MAC과 IP를 일명 DHCP sniffing 기법에 의해서 sniffing table에 보관한 뒤 ARP sniffing 공격에 대해 탐지 및 차단할 수 있는데, 동작 과정은 그림 15와 같다.

- DHCP 과정에서 관련 패킷을 sniffing 기법에 의해 획득한 후 MAC과 IP 정보를 포함한 DHCP sniffing table 생성
- 생성된 테이블 내용에 따라 permit ACL(Access Control List) 생성
- ARP 입력 시 내부 MAC과 IP 정보를 알기 위해 decapsulation 과정 수행
- 생성해 놓은 ACL에 의해 통과 및 차단 결정

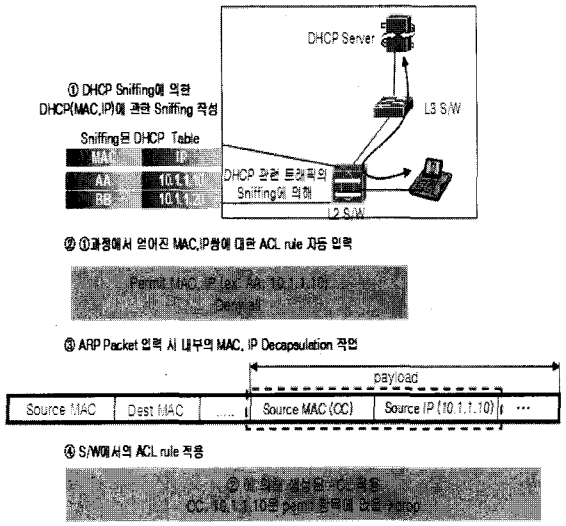


그림 15. DHCP Sniffing table과 ACL을 이용한 제안된 방어 방안
Fig. 15. Proposed protection scheme using DHCP sniffing table and ACL protection.

DHCP sniffing기법은 DHCP snoop binding 기법과는 다르게 가입자 L2 스위치가 DHCP relay기능을 한 후DHCP server로부터 정보를 받아서 필요한 정보만을 전달하는 방식이 아니라, DHCP 패킷 중 DHCP server로부터의 인증된 ACK 정보만 capture하여 decapsulation하는 기술을 이용하는 방법으로서 DHCP snoop binding 기법과 비교 시 다양한 장점이 있다.

- 생성된 DHCP table과 ARP table의 비교 과정 없이 바로 ACL을 만들어 입력되는 ARP 진위 여부를 결정함으로 한 동작 단계를 줄일 수 있어 장비의 부담을 줄일 수 있다.
- DHCP 정보의 중복 등록 문제 제거를 위해 스위치에서의 filtering 기법을 적용하지 않음으로 운용/관리가 용이하다.
- DHCP 패킷에 대해 서버 및 가입자로의 relay 기능을 제공하지 않아도 됨으로 개발이 용이하다는 점이다.

하지만 가입자의 MAC, IP 정보가 많아짐에 따라 적용해야 하는 ACL의 개수가 증가하여 룰 갯수가 제한

되어 있는 구 장비의 적용에는 한계가 있다는 단점이 있다.

2. ARP redirection 공격에 대한 대처 방안

가. ARP redirection 공격시 DHCP snoop 방법의 문제점

ARP spoofing 공격 대응 방안인 DHCP snoop이나 sniffing/inspection 기법을 ARP redirection 공격에 대한 대응방안으로 적용할 경우, 게이트웨이에 대한 정보가 L2 스위치의 DHCP relay DB에 없기 때문에 그림 16과 같이 적용이 불가하다. 따라서 DHCP snoop binding DB에 없는 게이트웨이 정보를 특정한 방법으로 관리, 운용하는 기법이 요구된다.

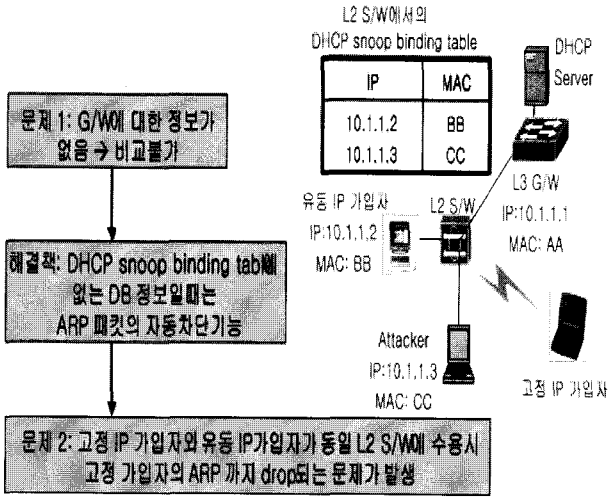


그림 16. 게이트웨이에 대한 DHCP snoop 기법 적용시 문제점

Fig. 16. Problem when applying DHCP snoop scheme on gateway.

나. Static Binding 기법

게이트웨이의 주소변조를 막기 위해서는 각 스위치에서 게이트웨이의 MAC과 IP 정보 등을 고정적으로 입력하고, 동적으로 들어오는 게이트웨이 MAC 정보는 무시하도록 하는 룰을 같이 적용해야만 완벽한 ARP redirection 공격에 대한 방어가 가능하다. 하지만 게이트웨이 위치는 각 L2 스위치보다 상위에 위치하고 있어, 게이트웨이에 대한 DHCP 트래픽 정보를 얻을 수 없기 때문에 ARP spoofing 공격 대처방안인 DHCP snoop 기능 적용만으로 해결될 수 없다.

따라서 그림 17과 같이 게이트웨이에 대한 정보를 수동으로 입력하여 DHCP binding table에 적용할 수

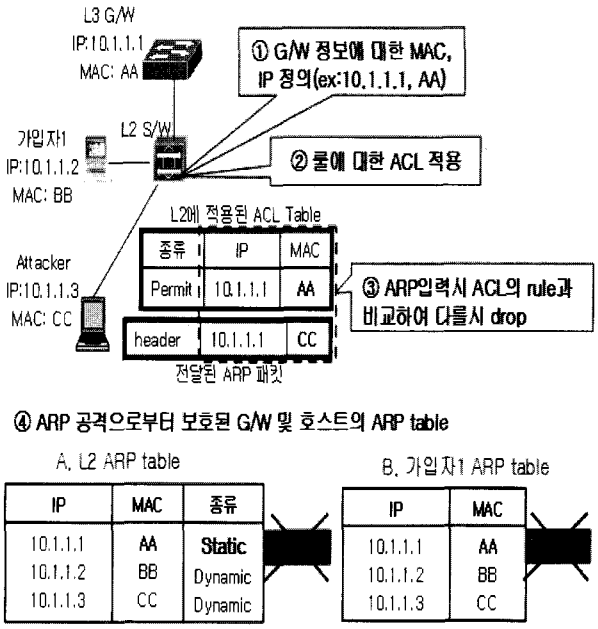


그림 17. Static binding 기법

Fig. 17. Static binding scheme.

있는 일명 static binding 기법을 적용하여 게이트웨이 자체의 MAC변조뿐 아니라 가입자로 향하는 왜곡된 게이트웨이에 대한 정보도 실시간으로 차단해야 ARP redirection 공격에 대해서도 방어할 수 있다. 생성된 table을 기반으로 IP와 MAC에 대한 ACL(Access Control List)이 작성되어 적용되며, ARP패킷 여부를 검토 후 ARP 패킷에 해당되면 decapsulation하여 DHCP binding table에 저장된 게이트웨이의 MAC 및 IP와 비교를 해서 허용 혹은 불허를 결정한다.

3. DOS형 ARP 공격에 대한 대처 방안

MAC 플러딩 공격은 한 포트에서 수 천 개의 호스트가 스위치와 연결되어 있는 것으로 보이지만 실제는 변조된 MAC 정보를 공격 호스트에서 발생시키는 것이며 연속된 ARP 패킷은 DOS(Denial Of Service)형태로 공

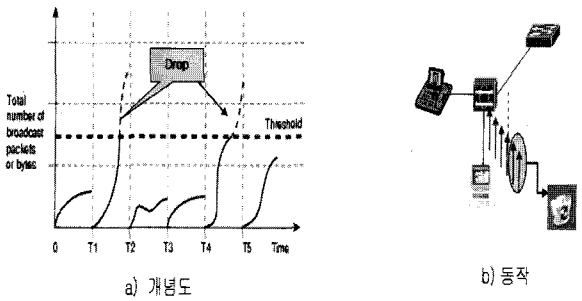


그림 18. ARP형 DOS(Denial Of Service) 공격 방지 방안

Fig. 18. The prevention scheme for ARP DOS attack.

격 대상자의 CPU등에 부하를 증가시켜 정상적인 서비스에 큰 지장을 줄 가능성도 있다[13].

따라서 그림 18에서 보는 바와 같이 임계값을 정해서 broadcast 패킷이 어느 이상 증가하면 폐기시킴으로써 네트워크 부하증가를 방지하고 네트워크 장비도 보호할 수 있다. 적용 기법으로 storm control 방식과 flood guard라는 방식이 있으며, 두 기능 모두 ARP broadcast 공격을 방어할 수 있다는 공통점이 있다. Storm control은 해당 broadcast 패킷에 대해서 포트 대역폭을 설정하여 패킷의 양을 조절하는 기법이며, flood guard는 1초 동안 수용할 수 있는 패킷 갯수를 제한하여 패킷을 조절하는 rate limit 기능을 이용하는 방법이다. 그림 19 a)와 같이 broadcast된 ARP 패킷의 총합이 지정된 임계값을 넘어가면 네트워크 및 장비 부하를 방지하기 위해 자동적으로 차단하는 기법을 적용하여 DOS형 ARP 공격으로부터 보호할 수 있다.

4. 전체 적용 기법

ARP 공격에 대해서 상향공격인 redirection 공격과 하향 공격인 spoofing 공격에 대해 별도의 대처방안을 제안하였고, 또한 DHCP broadcast 트래픽에 의해 발생하는 문제점에 대한 해결방안도 통합적으로 제시하였다. 즉, 그림 19와 같이 상향 공격인 ARP redirection 공격에 대해서는 게이트웨이 주소를 수동으로 적용하여 DHCP snoop 기능을 접목하는 기법인 일명 static binding 기술을 이용하여 차단할 수 있으며, DOS형 ARP 공격에 대해서는 threshold값을 정하며 입력 ARP가 이 임계값을 넘지 않도록 규정함으로써 ARP 공격을 차단할 수 있다.

적용순서로는 먼저 DHCP snoop 기능을 적용한 스위치에서의 DHCP 트래픽이 다른 L2 스위치로 전파되지 않게 하기 위해서 egress filtering 기술을 적용하고, 또한 DOS형 공격에 대비해 storm control 등의 임계치 기법을 적용한다. 이때 하향 ARP 공격은 DHCP snoop을 실행하고 상향 ARP 공격은 static binding 기법을 적용하며 DHCP 등록과정에서 생긴 MAC과 IP 정보에 의해 DHCP snoop binding table을 만들고, 이를 기반으로 허락된 ARP 패킷만 통과할 수 있도록 ACL(Access Control List)을 적용한다. 이후 ARP 패킷이 스위치로 입력 시 payload내의 MAC과 IP를 구분하기 위하여 decapsulation 작업을 시행하고, 이 정보를 기존에 생성한 ACL에 적용하여 허용된 IP와 MAC만을 가진 ARP 정보만이 broadcast domain 내부로 통과할

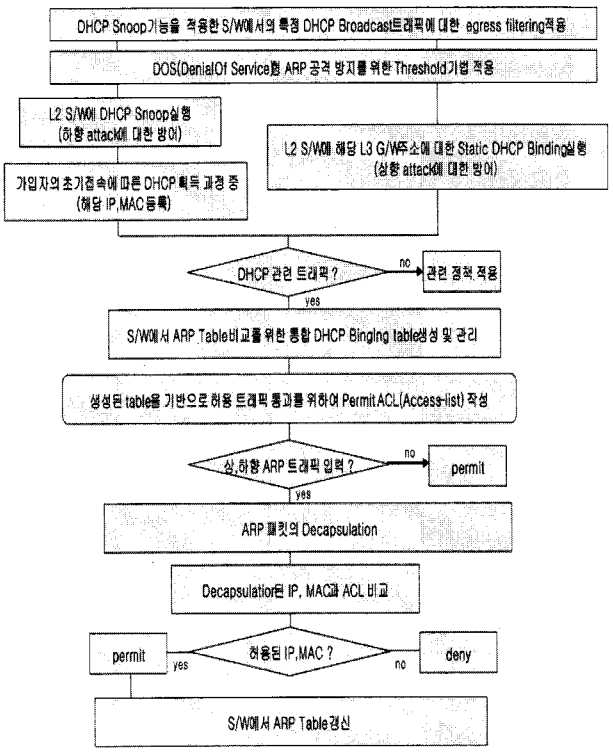


그림 19. ARP 공격 방어를 위한 세부 동작 순서도
Fig. 19. Detailed operation flow diagram to prevent ARP attack.

수 있도록 적용하여, 위조된 ARP response로부터의 테이블 변경을 사전에 차단할 수 있다.

V. 구현 및 시험 결과

ARP 공격에 대한 시험망을 구성 후 ARP 공격 트래픽을 발생시킨 후 게이트웨이 및 가입자의 ARP 변동

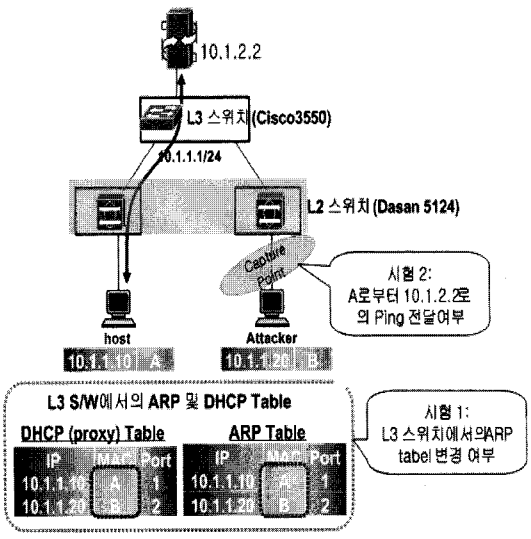


그림 20. ARP 공격 방어 유무 확인을 위한 시험구성도
Fig. 20. Testbed for the evaluation of ARP attack protection scheme.

1. G/W에서의 ARP Table 변화 여부

가. DHCP Snoop binding 기법을 적용하지 않을 경우 나. DHCP Snoop binding 기법을 적용 시

IP	MAC	Port
10.1.1.10	B	2
10.1.1.20	B	2

IP	MAC	Port
10.1.1.10	A	1

2. 공격자로의 트래픽 전송 여부 (Ping 이용)

가. DHCP Snoop binding 기법 적용 전

Source	Destination	Flags	Size	Absolute Time	Protocol	Summary
IP=10.1.1.10	IP=10.1.2.2		78	20:07:30.623382	PING Req	Echo: 10.1.2.2
IP=10.1.1.12	IP=10.1.2.2		78	20:07:30.623915	PING Req	Echo: 10.1.2.2
IP=10.1.2.2	IP=10.1.1.10		78	20:07:30.638343	PING Reply	Echo Reply: 10.1.1.12
IP=10.1.2.2	IP=10.1.1.10		78	20:07:30.638773	PING Reply	Echo Reply: 10.1.1.12

나. DHCP Snoop binding 기법 적용 후

Source	Destination	Flags	Size	Absolute Time	Protocol	Summary

그림 21. ARP snoop binding 기법에 대한 시험 결과값
Fig. 21. Test result of ARP snoop binding scheme.

유무 및 위조된 ARP response 트래픽이 네트워크상으로 전달되는지를 DHCP snoop binding 기법 및 static binding 기법을 적용 후 실험을 통해서 알아보았다.

그림 20은 시험망 구성도로서 호스트와 공격자를 별도의 L2 스위치(다산 5124)에 연결한 후 ARP 방어기법을 적용하지 않은 경우와 적용한 경우를 구분하여 시험하였고, 일반 가입자에서 인터넷으로 향하는 트래픽이 공격자를 경유하는지 여부를 확인하기 위해서 ping을 이용하였다. 또한 L2 스위치의 ARP 테이블 변경 유무를 차단기법 적용전과 후로 구분하여 측정하였다.

그림 21과 같이 DHCP snoop 기능을 적용하지 않을 때에는 L2 스위치의 ARP 테이블의 변경이 일어나 ping 트래픽이 공격자를 경유하여 지나가지만 적용시에는 ARP 테이블의 변경이 일어나지 않아 공격자를 경유하지 않고 통신함으로써 가로채기 공격 등으로부터 보호됨을 확인할 수 있다.

VI. 결론 및 향후 연구사항

1. 고정 IP 가입자의 ARP 공격에 대한 대처 방안

가입자 환경이 DHCP IP 할당방식이 아니라 고정 IP 방식일 경우 ARP 공격 차단기법으로 DHCP snoop 방식을 사용할 수 없다는 문제가 발생되며, 따라서 DHCP 정보를 이용하는 것과는 다른 기법이 필요하다. 이를 위해 그림 22와 같은 인증서버와의 연동방식이 필요하며 동작순서는 다음과 같다.

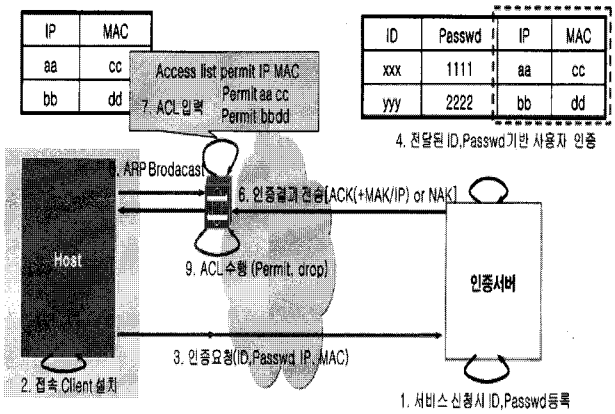


그림 22. AAA 서버와의 연동을 통한 ARP 공격 방어 대책
Fig. 22. The ARP attack protection scheme using AAA server.

- 인증 서버에서 사용자에게 할당된 IP/MAC 값을 인증 DB의 필드값에 저장
- 가입자 스위치는 단말로부터의 인증 요청시 단말의 MAC 정보를 받아 AAA server로 ID/Password 값과 함께 MAC/IP 정보를 전달
- 가입자 접속 스위치는 AAA server와 연동하여 IP, MAC에 대한 정보를 일명 ARP-AAA table에 저장
- AAA client인 가입자 L2 스위치는 AAA 서버와 연동하여 해당 가입자에 대한 ACL(Access Control List)를 작성 및 적용
- 스위치는 ARP 패킷 입력 시 패킷을 decapsulation 하여 MAC과 IP 정보를 추출
- 이 추출된 정보를 ARP-AAA table에 저장된 MAC/IP 정보와 비교 후 동일하며 허용하고 틀리면 거절하여 ARP 공격 packet이 네트워크상으로 통과되는 것을 방지하여 안정성을 보장

이 기법은 고정가입자 및 유동 가입자 모두 적용 가능하고 향후 단말 인증 서비스 제공 시 MAC을 기준값으로 연동하여 사용 가능하다는 장점이 있지만, 가입자 스위치에서 단말 MAC 정보를 받아서 server로 전달하는 relay 기능을 제공하여야 하고, 인증서버에서 인증 정보 관리 외에 인증 성공 후 ACK 전송 시 해당 MAC/IP를 전송하는 별도 과정이 필요하므로 서버의 부하 문제/성능 및 안정성이 검증되지 않았다는 단점이 있어서 이에 대한 향후 연구가 필요하다.

2. 분리된 VLAN 인터페이스 구성 및 운용 기법

L2 장비의 다양성 및 장비 성능 제한으로 앞에 기술

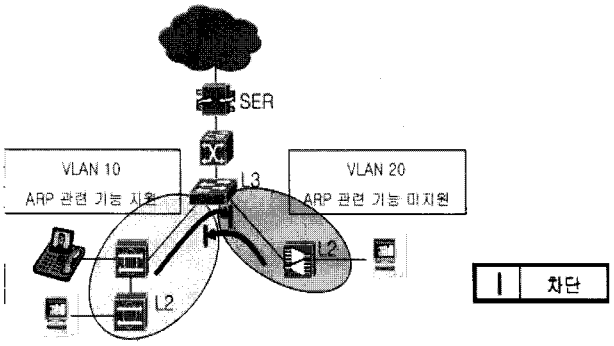


그림 23. 분리된 VLAN 인터페이스 구성 및 운용
Fig. 23. The Configuration and operation with separated VLAN interface.

된 DHCP snoop 및 static binding기능이 적용될 수 없는 장비가 있을 수 있으며 이로 인해 기능 제공 장비와 미 제공 장비가 동일 L3 스위치 내에 수용된 경우 미 제공 장비로부터 시작된 ARP 공격이 기능 제공 장비에 수용된 가입자의 ARP 테이블을 변경시킬 수 있다.

따라서 그림 23과 같이 ARP 차단 기능을 제공하는 L2 스위치에 수용된 가입자 그룹과 적용되지 않은 L2 스위치 그룹을 별도의 VLAN 인터페이스에 수용시킴으로써 서로의 영향을 주지 않고, 장비 대체 및 기능 업그레이드가 될 때까지 독립성을 유지하며 동작시킬 수 있다.

3. 결 론

본 논문은 향후 네트워크 공격으로 심각한 영향을 끼칠 것으로 예상되는 ARP 공격에 대해서 실제로 시험을 통하여 취약점 및 심각성을 분석하였으며, 이를 방어하기 위해서 현재 네트워크 장비에서 제공되는 기술의 조합을 통한 방안뿐 아니라 새로운 보안기법을 제안하였다.

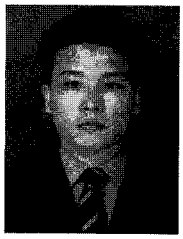
기존 연구들은 프로토콜 자체 보안을 위해 한 쌍의 키를 사용하는 S-ARP(Secure ARP) 방안과 네트워크 장비 기술을 이용하는 방안으로 나누어 볼 수 있으나, 두 방안 모두 일시적이고 단편적인 문제만을 해결할 뿐 다양한 공격 시나리오 상황에서 완벽하게 대처할 수 없어서 적용이 어려운 기법이라 할 수 있다.

본 논문에서 제안한 IP 할당과정에서의 DHCP 정보를 이용하는 DHCP snoop binding 기법 및 static binding 기법 등은 ARP 공격에 대한 완벽한 탐지 및 차단은 물론 향후 BcN 네트워크가 QoS, 토폴로지 관리, 단말 인증 등을 위해서 고정 IP 할당방식에서 DHCP 방식인 유동 IP 할당 방식으로 변환하는 시점에서 그 범용성과 미래 실행 가능성이 어느 기법보다 높고 정확한 대안이라 할 수 있다. 따라서 이 논문에서 제안한 ARP 공격에 대한 보안 기법은 BcN을 비롯한 차세대 인터넷 접속망의 보안성을 강화하는데 널리 사용될 수 있을 것이다. 이와 더불어 향후 topology 관리, QoS, multicast 등과의 연관성 등에 대한 보안 연구가 필요할 것이다.

참 고 문 헌

[1] William Stallings, "Network Security Essentials Application and Standards Second Edition", 2002.
[2] 정진욱, 김현철, 조상홍, "컴퓨터 네트워크" 생능출판사, 2002.
[3] Fred Halsall, "Data Communications, Computer Networks and Open Systems", ADDISON WESLEY, 1996.
[4] Address Resolution Protocol, RFC 826: http://www.ietf.org/rfc/rfc903.txt.
[5] 최원우, 정진욱, 안성진, "A Study on Network Security Problems Analysis of ARP Mechanism", 한국 응용 수학회, Aug 2004.
[6] Hastings, N.E, TCP/IP spoofing fundamentals, Computers and Communications, 1996, Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference (1996) 218-224.
[7] Miscellaneous Security: hacking tools. http://www.experts-exchange.com/Security/Misc/Q_21287353.html.
[8] S. Kent and R. Atkinson, Security architecture for th Internet Protocol, RFC 2401, 1998.
[9] M. Laubach. "Classical IP and ARP over ATM" RFC1577, Jan.1994.
[10] A. Householder and B. King. Securing an internet name server. http://www.cert.org/archive.
[11] Dynamic Host Configuration Protocol (RFC 1531): http://www.ietf.org/rfc/rfc1531.txt.
[12] DHCP Relay Agent Information Option (RFC 3046): http://www.ietf.org/rfc/rfc3046.txt.
[13] Sanjeev Kumar, IEEE Senior Member, USA, Impact of Distributed Denial of Service (DDoS) Due to ARP Storm.

저 자 소 개



오 석 환(정회원)
정보통신기술사(Professional Engineer Information), CCIE (Cisco Certified Internetwork Expert)
2007년 충남대학교 정보통신공학과 석사
1995년~현재 (주)KT 선임연구원
<주관심분야 : WiBro, BcN, 네트워크 보안>

김 병 철(종신회원)
1988년 서울대학교 전자공학과 학사
1990년 한국과학기술원 전기 및 전자공학과 석사
1996년 한국과학기술원 전기 및 전자공학과 박사
1993년~1999년 삼성전자 CDMA 개발팀
1999년~현재 충남대학교 정보통신공학부 부교수
<주관심 분야 : 이동인터넷, 이동통신 네트워크, 데이터통신>

이 재 용(종신회원)-교신저자
1988년 서울대학교 전자공학과 학사
1990년 한국과학기술원 전기 및 전자공학과 석사
1995년 한국과학기술원 전기 및 전자공학과 박사
1990년~1995년 디지콤 정보통신연구소 선임연구원
1995년~현재 충남대학교 정보통신공학부 교수
<주관심분야 : 초고속통신, 인터넷, 네트워크 성능분석>