KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.4 pp.203~210 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.4.203

Address Auto-Resolution Network System for Neutralizing ARP-Based Attacks

RhongHo Jang[†] · KyungHee Lee[††] · DaeHun Nyang[†††] · HeungYoul Youm[††††]

ABSTRACT

Address resolution protocol (ARP) is used for binding a logical address to a physical address in many network technologies. However, since ARP is an stateless protocol, it always abused for performing ARP-based attacks. Researchers presented many technologies to improve ARP protocol, but most of them require a high implementation cost or scarify the network performance for improving security of ARP protocol. In this paper, we present an address auto-resoultion (AAR) network system to neutralize the ARP-based attacks. The AAR turns off the communication function of ARP messages(e.g. request and reply), but does not disable the ARP table. In our system, the MAC address of destination was designed to be derived from destination IP address so that the ARP table can be managed statically without prior knowledge (e.g., IP and MAC address pairs). In general, the AAR is safe from the ARP-based attacks since it disables the ARP messages and saves network traffics due to so.

Keywords : ARP Spoofing, ARP Message Disable, Static ARP Lable, Network Bandwidth Saving, MAC Address Derivation

ARP 기반 공격의 무력화를 위한 주소 자동 결정 네트워크 시스템

장 룡 호[†] · 이 경 희[††] · 양 대 헌[†††] · 염 흥 열[††††]

요 약

주소 결정 프로토콜, ARP(Address Resolution Protocol)는 네트워크의 논리 주소(IP)로부터 물리 주소(MAC)를 찾아내는 프로토콜로 많은 네트워크에 사용되고 있다. 그러나 ARP는 메시지 내용의 진위를 검증할 수 있는 수단이 없기 때문에, 이를 이용한 공격이 많이 이루어지고 있다. 많은 연구자들이 ARP의 안전성을 보완하는 많은 기술들을 제안하였지만, 대부분은 ARP의 안전성을 향상하는 대신에 네트워크의 성능을 희생하거나 많은 구현 비용을 요구한다. 이 논문에서는 ARP 기반의 공격을 무력화하는 AAR(Address Auto-Resolution, 주소 자동 결정) 네트워크를 제안한다. AAR에서는 기존의 ARP 테이블을 사용하지 않는 것이 아니라 요청(request), 응답(reply) 등 기본적인 ARP 메시지를 사용하지 않으며, MAC 주소를 IP 주소로부터 유도할 수 있도록 설계하여 ARP 테이블을 사전지식(IP, MAC 주소의 쌍) 없이 정적으로 관리할 수 있게 한다. 이 시스템은 기본적인 ARP 메시지 기능을 차단하므로 ARP 기반의 공격을 무력화할 수 있는 동시에 네트워크 트래픽을 절약하는 효과도 있다.

키워드 : ARP 스푸핑, ARP 메시지 차단, 정적 ARP 테이블, 네트워크 트래픽 절약, MAC 주소 유도

1. 서 론

ARP(Address Resolution Protocol)은 데이터 링크 계층에서 네트워크의 논리 주소(IP 주소)를 물리 주소(MAC 주소)로 바인딩 하는 프로토콜이다. 정상적으로 네트워크 통신이 이루어지기 위해서는 호스트들의 IP들과 MAC 주소를 바인딩 하여 저장하는 ARP 테이블(캐시)이 필요하며 ARP 요청(request) 및 응답(reply) 메시지에 통해 관리된다. 그러나 ARP 메시지는 누가 보냈는지를 검증할 수 있는 수단이 없기 때문에, 만약 같은 네트워크에 있는 호스트가 변조된 ARP 메시지를 보낼 경우 그 메시지를 받은 사용자는 잘못된 MAC 주소로 데이터를 보내게 된다. 이를 이용하여 ARP 스푸핑(spoofing) 공격을 수행할 수 있으며, 성공했을 경우 피해자는 중간자(Man-in-the-Middle) 공격 등 다양한 보안 위협에 노출되게 된다. ARP 스푸핑 공격은 오래된 네트워크 보안 이슈임에도 불구하고, 공격을 수행하기 위해서 많

※ 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. R0127-16-1051, IoT 환경에서 프라이버시 보호 국제 표준화).
† 준 회 원 : 인하대학교 컴퓨터공학부 박사과정
†††† 종신회원 : 수원대학교 전기공학과 부교수
††† 정 회 원 : 인하대학교 컴퓨터정보공학과 교수
†††† 비 회 원 : 순천향대학교 정보보호학과 정교수
Manuscript Received : January 18, 2017
First Revision : February 8, 2017
Accepted : February 20, 2017
* Corresponding Author : HeungYoul Youm(hyyoum@sch.ac.kr)

은 전문적인 지식이 필요하지 않으며 공격에 필요한 소프트웨어도 인터넷을 통해 쉽게 찾을 수 있으며, 공격 사례도 쉽게 찾을 수 있다[1]. 현재까지 ARP 스푸핑 공격을 탐지 및 방어하기 위해 SARP[2], ASA[3], Invite-accept[4] 등 다양한 기술들이 제안 되었지만, 이들은 높은 구현 비용을 요구하거나 네트워크 성능을 희생하여 보안성을 향상하는 경우가 대부분이다. 이런 이유에서 ARP 공격에 대한 연구가 아직까지도 지속적으로 진행하고 있다[5-11].

이 논문에서는 ARP 기반의 공격을 무력화하기 위한 주소 자동 결정(AAR, Address Auto-Resolution) 네트워크를 제안한다. 이 시스템에서는 동적 ARP 테이블 대신 정적 ARP 테이블을 사용하고, ARP 메시지를 사용하지 않기 때문에 ARP 메시지 기반의 공격을 무력화한다. 정적 ARP 테이블을 사용하려면 네트워크의 모든 호스트들의 IP 주소와 MAC 주소의 쌍에 대한 정보가 필요하지만, 이 시스템에서는 MAC 주소를 IP 주소로부터 유도할 수 있도록 설계하여, 정보 수집을 위한 인력 낭비가 발생하지 않는다. 부가적으로 ARP 메시지를 사용하지 않기 때문에, ARP 메시지가 사용하던 네트워크 트래픽을 절약할 수 있다.

2. 위협 모델 및 관련 연구

2.1 위협 모델

네트워크 사용자는 네트워크에 있는 다른 디바이스들과 통신하기 위해서 디바이스들의 논리 주소(IP 주소)뿐만 아니라 해당 주소를 사용하는 네트워크 디바이스의 물리 주소(MAC 주소)도 알아야한다. 이러한 IP 주소와 MAC 주소의 바인딩 정보들은 캐시 형태로 ARP 테이블에 저장이 되고, ARP 요청 및 응답을 통해 관리된다. ARP 요청은 특정 IP 주소를 가진 디바이스의 MAC 주소 정보를 요청하는 메시지이며 네트워크의 모든 디바이스에게 전송한다. 해당 정보를 가지고 있는 디바이스는 ARP 응답 메시지로 응답한다.

현재 사용 중인 ARP는 ARP 요청 및 응답 메시지 내용에 대한 검증을 수행하지 않고 있다. 따라서 어떤 사용자가 악의적으로 ARP 응답 메시지에 잘못된 정보를 담아 응답하면, 정보를 요청한 주체는 잘못된 IP 및 MAC 주소의 바인딩 정보를 ARP 캐시 테이블에 저장하여 다른 사용자한테 데이터를 보내게 되는데, 이러한 공격을 ARP 스푸핑(spoofing)이라고 한다.

Fig. 1은 ARP 스푸핑을 이용한 중간자(Man-in-the-Middle) 공격을 설명하고 있다. 공격자 PC-3가 PC-2에게 게이트웨이의 MAC 주소는 MAC-3이라고 지속적으로 응답하면서, 게이트웨이에게 PC-2의 MAC 주소가 MAC-3이라고 지속적으로 응답하면, PC-2와 게이트웨이의 ARP 캐시 테이블은 잘못된 정보로 업데이트 된다. 즉, PC-2와 게이트웨이는 서로에게 보내야하는 데이터를 모두 공격자 PC-3에게 보내게 되며, 공격자는 패킷 릴레이(relay) 기능을 수행하면서 PC-2와 게이트웨이의 통신을 도청할 수 있다.

이러한 ARP 기반의 공격을 방어하는 기법들은 암호학적

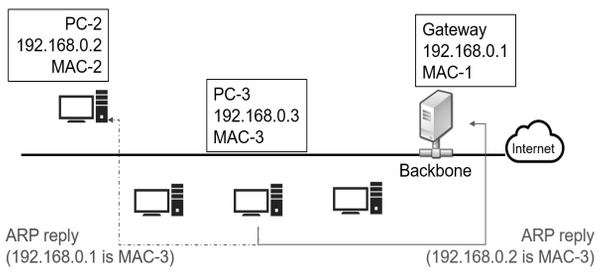

Fig. 1. Example of Man-in-the-Middle Attack Using ARP Spoofing

(cryptographic) 또는 비암호학적(non-cryptographic) 접근으로 분류할 수 있다. 암호학적 접근 방법은 표준 ARP의 구조를 변경하여 사용하는 것이 특징이며 암호화 및 복호화 등 기능을 추가적으로 수행하기 때문에 비암호학적 접근 방법보다 더 많은 연산이 필요로 한다. 비암호학적 접근 방법은 표준 ARP의 구조를 변경하지 않아 구현이 상대적으로 용이하다.

2.2 암호학적 방어 기법

SARP(Secure ARP)는 공개키(public key) 기반의 ARP 인증 시스템이다[2]. SARP에서는 모든 호스트가 자신의 IP 주소와 공개키를 AKD(Authoritative Key Distributor)에게 전달하며, AKD는 호스트들의 요청에 따라 IP 주소에 해당하는 공개키를 알려준다. AKD를 구성하기 위해서는 추가적인 장치가 필요하며, 비교적 더 많은 계산이 요구된다.

ASA(Agent-based Secure ARP)는 암호화된 UDP(User Datagram Protocol) 패킷을 ARP 패킷 대신 이용하여 ASA 에이전트들 사이에서 ARP의 역할을 수행한다[3]. ASA 에이전트에 저장되어있는 암호화된 정보는 ARP 테이블을 업데이트 하는데 사용된다.

2.3 비암호학적 방어 기법

Gouda 등은 ARP 프로토콜 외에 초대 수락(invite-accept) 프로토콜을 추가적으로 사용하는 방법을 제안하였다[4]. 초대 수락 프로토콜은 이더넷 통신을 하는 모든 호스트에서 동작하며 IP 주소와 MAC 주소 쌍의 유효성을 검증한다. 이 기법은 추가적인 프로토콜을 사용하기 때문에 더 많은 네트워크 대역폭 및 CPU 자원을 소모한다.

TARP(Ticket-based ARP)는 사용자가 LTA(local ticket agent)로부터 IP 주소와 MAC 주소의 쌍으로 이루어진 서명된 티켓을 발급받아서 ARP 응답메시지에 첨부하는 방식이다[5]. 첨부된 티켓은 서버에서 주소의 유효성을 검증하는 용도로 사용이 된다.

Enhanced ARP는 투표(voting) 기반의 방식으로 ARP 정보를 인근에 위치한 여러 사용자들로부터 모으는 방법을 사용한다[6]. 중복으로 ARP 메시지를 보내기 때문에 네트워크 성능에 영향을 준다.

PARP(Probe-based ARP)는 ARP 응답 메시지를 받으면 메시지 보낸 호스트한테 즉시 ICMP 에코 요청(echo request) 메시지를 보내, 응답여부에 따라 공격자인지를 판단한다[7].