신뢰적인 ARP Table의 운영을 통한 ARP Spoofing 공격에 대한 효율적인 방어 기법*

홍승표[O1] 오명진[2] 이수연[3] 이상준[1]
[1]숭실대학교 컴퓨터학부
[2]고려대학교 컴퓨터통신공학부
[3]동덕여자대학교 컴퓨터학과
hsp0515@gmail.com, iamOhMj@gmail.com, srksyd@naver.com, sangjun@ssu.ac.kr

An Efficient Prevention Technique using operating the Reliable ARP Table for ARP Spoofing Attacks

Seungpyo Hong[O1] Myeongjin Oh[2] Suyeon Lee[3] Sangjun Lee[1]
[1]School of Computing, Soongsil University
[2]Division of Computer and Communication Engineering, Korea University
[3]Department of Computer Science, Dongduk Women's University

네트워크의 눈부신 발전과 더불어 전 분야에서 인터넷의 활용도가 증가하고 있다. 특히 인터넷이 제공하는 편의성, 접근성, 그리고 상업성으로 인해 인터넷의 의존도는 점점 더 높아져 가고 있다[1]. 이러한 의존도는 보안상의 취약함이 드러날 때 큰 문제를 야기할 수 있다. 특히 ARP(Address Resolution Protocol)의 보안상 취약점으로 인한 ARP Spoofing 공격 사례가 급증하고 있어 이에 대한 대비책이 시급한 실정이다.

ARP 프로토콜의 취약점이 처음 발견된 1982년으로부터 근 30년이 지났지만 최근까지도 ARP Spoofing을 이용한 피해사례가 빈번하게 발생하고 있다[2]. 이는 오랜 기간에 걸쳐 여러 방어 기법들이 제안되었음에도 불구하고 전반적으로 적용되고 있지 못함을 보여준다. 특정 방어 기법의 경우 고가의 장비가 필요한 이유로 일부 기관에만 한정적으로 설치되어 운영되고 있으며, 일반적으로 공개된 지역에서는 이에 대한 대책 없이 무방비 상태로 방치된 곳이 대부분이다. 실제로 2008년 7월 국내에서 ARP Spoofer에 의한 피해 사례는 보고된 것만 141건으로 전체의 15.6%를 차지하였다[3].

ARP 프로토콜은 데이터를 전송하기 전에 타겟 IP 주소에 해당하는 MAC주소가 ARP Table에 없을 때, ARP 요청을 브로드캐스팅 한다. 같은 서브넷 안에 모든 호스트는 브로드캐스팅 된 ARP 요청에 해당하는 IP 주소가 해당 호스트의 IP일 경우, ARP 응답을 통해 MAC주소를 요청한 호스트에 알려준다. 이러한 일련의 과정이 상호 간의 인증 없이 이루어지기 때문에 문제가 발생할 수 있다. 이러한 취약점을 이용하여 악의적인 사용자가 정상 사용자들의 MAC주소를 자신의 MAC주소로 변조하면 정상 사용자들 간에 데이터 전송은 악의적인 사용자를 통해 이루어지게 되고 모든 데이터는 스니핑될 수 있다.

기존 연구를 살펴보면 현재의 ARP 프로토콜 자체를 수정하거나 별도의 하드웨어 장비를 사용한 방어 기법이 대부분이며 현실에 적용하기에는 어려움이 있다. 이와 더불어 별도의 장비를 필요로 하지 않고 ARP Table을 정적으로 유지하여 MAC 주소의 조작을 막는 기법은 이미 알려져 있지만, 관리자가 로컬 망의 모든 호스트들의 주소를 수작업으로 입력해야 하기 때문에 규모가 큰 네트워크 환경이나 DHCP 환경에서는 현실적으로 불가능하다. 본 논문에서는 사용자를 ARP Spoofing 공격으로부터 보호하기 위해 신뢰할 수 있는 정보를 자동으로 ARP Table에 갱신하는 방법을 제안한다. 로컬 네트워크 망의 모든

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2008-C1090-0803-0006).

호스트가 정적 ARP Table을 자동으로 유지하도록 함으로써 ARP 프로토콜의 취약한 점을 근본적으로 제거한다.

본 논문이 제안하는 ARP Spoofing 방지 기법은 실제 프로토콜의 변경이 없기 때문에 기존 호스트들 간에 네트워크를 사용하는데 제한이 없다. 이는 사용자의 이동이 잦은 환경에서도 시스템을 구축 가능하게 할 수 있다. 본 시스템은 크게 사용자 PC의 ARP Table을 ARP Spoofing 공격으로부터 보호하는 Client-Agent와 신뢰적인 ARP Table을 보관 및 갱신을 위한 MAC-Agent로 구성되어 있다. 본 시스템을 실제 적용하기 위해 서브넷 안에 하나의 MAC-Agent를 제공해야 하며, 이는 일반 PC에서 쉽게 동작되며, Spoofing 공격으로부터 보호 받고 싶은 사용자는 Client-Agent를 설치하여 사용하면 된다.

Client-Agent는 어플리케이션과 커널 영역에서 동작하는 디바이스 드라이버[4]로 구현하였으며, 일반적으로 많이 사용되는 운영체제인 Windows XP와 Windows 7에서 개발하였다. Client-Agent의 어플리케이션은 MAC-Agent가 전송한 ARP Table 정보를 보관한다. 만약 사용자가 ARP Table에 없는 IP주소로 전송을 시도하면 어플리케이션이 갖고 있는 신뢰적인 주소 목록을 검색하여 신뢰할 수 있는 IP일 경우 해당 MAC 주소를 ARP Table에 정적으로 갱신한다. 정적으로 갱신 된 주소는 기존 프로토콜이 동적으로 동작하는 방식과 동일하게 20분 주기[5]로 삭제된다. 이는 ARP Table의 크기를 조절하여 일반적으로 사용되는 C class 외에도 B class와 A class와 같이 서브넷이 큰 환경에도 적용 가능하게 한다. Client-Agent의 디바이스 드라이버는 NIC 위에서 동작하며 들어오고 나가는 패킷을 분석하여 ARP 요청이나 응답을 필터링하는 역할을 수행한다.

Client-Agent에 의해 모든 호스트의 ARP Table은 보호되지만 게이트웨이 장비 자체에는 본 시스템이 구축되어 있지 않기 때문에 게이트웨이의 ARP Table은 별도로 보호해야 한다. 왜냐하면 게이트웨이의 ARP Table 역시 ARP 응답에 의해 사용자 인증 없이 변경 가능하고, 이를 이용하여 게이트웨이를 통하여 들어오는 데이터를 악의적인 사용자가 Spoofing 할 수 있기 때문이다. 그러나 펌웨어로 동작하는 게이트웨이의 ARP Table을 외부에서 Static으로 고정시킬 수 없기 때문에 주기적으로 게이트웨이 ARP Table의 변조 여부를 확인해야 한다. MAC-Agent는 Client-Agent를 통해 구축된 신뢰적인 주소를 ARP 요청으로 브로드캐스팅하고, 게이트웨이에서 전송된 MAC주소를 이미 알고 있는 MAC 주소와 비교하여 변조유무를 확인한다. 본 시스템은 서버와 클라이언트의 어플리케이션 Layer 간에 신뢰할 수 있는 ARP Table을 안전하게 주고받기 위해 암호화를 수행한다. 기준 시간으로부터 일정 시간마다의 타임스탬프 값에 SHA-1 해시 알고리즘을 적용한 결과 값을 Key 값으로 하여 AES[6] 암호화 알고리즘으로 데이터를 보호한다.

본 논문에서는 실험을 통하여 ARP Spoofing 공격으로부터 사용자를 보호하는 것을 보였다. 물리적으로 분리된 PC에 MAC-Agent가 별도로 필요하나 이는 가벼운 어플리케이션이며 프로토콜의 수정 및 고가의 장비 없이 ARP Spoofing 공격을 막는 호스트 기반의 방법으로써 현재 네트워크에 적용 가능한 기법이다.

참고문헌

[1] S.Garfinkel. Web Security and Commerce. O'Reilly & Associates, Cambridge, 1997.

[2] http://www.ahnlab.com/kr/site/securitycenter/asec.

[3] http://company.hauri.co.kr/news/security_news_view.html?intSeq=1408&no=.

[4] http://en.wikipedia.org/wiki/Network_Driver_Interface_Specification.

[5] W.Stevens and R.Wright, TCP/IP illustrated (vol. 2): the implementation, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 1995.

[6] J. Daemen and V. Rijmen. The Design of Rijndael: AES-The Advanced Encryption Standard, Springer-Verlag,BerlinGermany, 2002.