Local Area Network상의 ARP Redirect attack 대응 모델에 관한 연구

*이선중,*김정문,*예홍진
*아주대학교 정보통신전문대학원
e-mail:(plantiff, kjm517, hjyeh)@ajou.ac.kr

Study Response Model against ARP Redirect attack on Local Area Network

Sun-Joong Lee, Jung-Moon Kim, Hong-Jin Yeh
Graduate School of Information Communication ,
Ajou University

요 약

하나의 물리 망 위에 있는 두 시스템은 상대방의 물리 주소를 알고 있어야만 통신을 할 수 있고, 물리 주소는 통신비용 절감을 위해 ARP를 사용하는 HOST의 ARP cache에 Internet-to-Ethernet Mapping형태로 저장한다. 이러한 ARP cache 구조는 Modification의 많은 취약성을 가진다. 그 중 취약성을 이용한 공격 중 하나인 ARP Redirect Attack은 물리 망 위의 Target Host 패킷이 공격자의 시스템을 통해 게이트웨이까지 가도록 한다. 본 논문은 게이트웨이 및 일반 HOST 시스템으로 구성된 Local Area Network 기반 구조를 내부 공격자 시스템으로부터 다른 내부 시스템의 사용자 정보를 안전하게 게이트웨이까지 보내기 위한 대응 모델을 제안하고자 한다.

1. 서론

물리적인 네트워크에서 두 개의 노드는 서로 물리적 주소를 알아야만 통신이 가능하다. Local Area Network(이하 LAN)상에서 HOST는 인터넷을 하기 위해 게이트웨이까지 가야한다. 그러나 게이트웨이의 IP 주소는 알고 물리적 주소를 알지 못하는 경우 게이트웨이까지 가기 위해 ARP Request 패킷을 Broadcast 하고 ARP Reply 패킷을 Unicast로 받게 된다. 이때 통신의 비용을 절감하기 위해서 HOST들은 최근에 Broadcast 되었던 ARP를 통해 Internet-to-Ethernet 묶음인 바인딩 내용을 ARP cache에 유지함으로써 ARP를 자주 사용할 필요가 없도록 하고, 이때 점점 커지는 cache를 유지하기 위해 일정기간 사용되지 않는 entry를 제거한다[1].

하지만 ARP는 LAN상의 HOST들이 게이트웨이에 대한 ARP Request Broadcast 후 공격자 HOST가 위조된 게이트웨이 ARP 패킷을 네트워크에 주기적으로 보내면, LAN상의 모든 HOST ARP cache는 위조된 Internet-to-Ethernet값을 자신의 cache에 저장하게 되는 보안상의 취약점을 가지고 있다. 이로서 피해 HOST들은 공격 시스템을 통하여 게이트웨이로 가게 되고 공격자는 필요한 피해 HOST 사용자 정보를 가질 수 있게 된다.

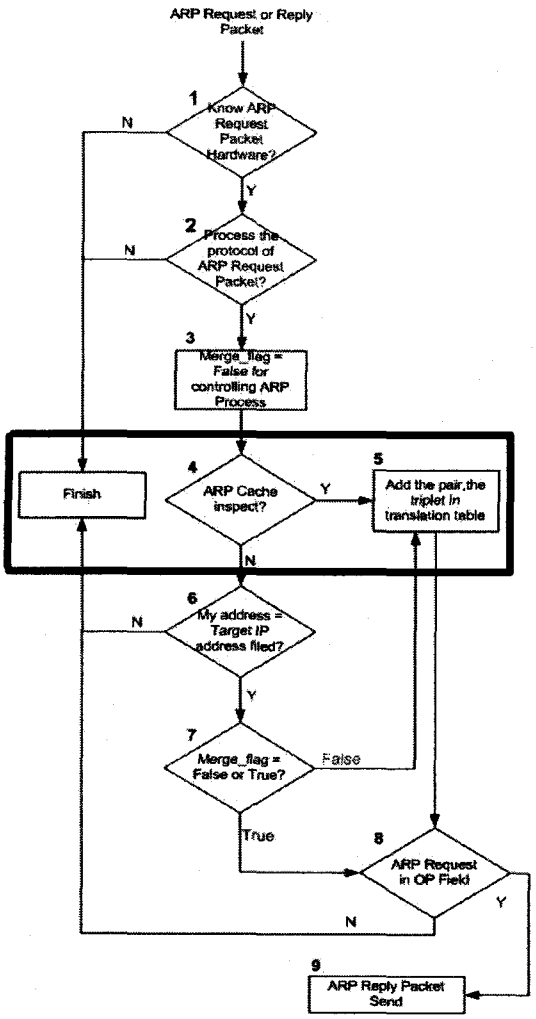
따라서 본 논문에서는 공격 시스템이 LAN상에서의 행해질 수 있는 DoS(denial of service)와 ARP Redirect Attack 통한 공격자 시스템으로부터 다른 내부 HOST 시스템의 사용자 정보를 안전하게 게이트웨이까지 보내기 위한 대응 모델을 제안 하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 ARP에 관련된 내용을 알아보고 3장에서는 LAN상에서 ARP를 이용한 공격 유형을 알아보고 4장에서는 본 논문의 기반을 이루는 대응 모델의 개요와 모델을 알아본다. 마지막으로 5장에서는 결론과 향후 과제에 대해 언급한다.

2. ARP

2.1 ARP(Address Resolution Protocol)

ARP는 IP 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜이다. 여기서 물리적 네트워크 주소라 함은 Ethernet 또는 토큰링의 48bits 네트워크 카드 주소를 말한다.



[그림 1- ARP 패킷 처리과정]

<그림 1 동작과정>

① HOST는 ARP request packet의 hardware종류를 알고 있는가? Yes면 다음으로 No이면 삭제.

② HOST는 ARP request packet의 프로토콜을 처리할 수 있는가? Yes면 다음으로 No이면 삭제.

③ ARP처리를 제어하기 위해 Merge_flag를 false로 설정한다.

④ ARP cache에 (프로토콜 종류, 송신자 프로토콜 주소)가 있는가?

이미 있으면 항목의 송신자 하드웨어 주소 필드를 패킷의 새 정보로 갱신하고 Merge_flag를 true로 설정한다. 아니면 다음으로 단계로 넘어간다.

⑤ 나의 주소가 대상 IP주소 필드의 것과 같은가? Yes면 다음으로 No이면 삭제.

⑥ Merge_flag가 false인지 확인한다.

⑦ Merge_flag가 false이면 (프로토콜 종류, 송신자 프로토콜 주소, 송신자 하드웨어 주소)을 변환테이블에 추가한다.

⑧ 작동(operation code) 필드에 ARP요청으로 나타나는가? Yes면 다음으로 No이면 삭제.

⑨ 하드웨어 필드와 프로토콜 필드를 맞바꾸어 지역 하드웨어와 프로토콜 주소를 송신자 필드에 넣는다. 작동 필드를 ARP reply로 설정한다. 패킷 요청을 수신한 것과 같은 하드웨어의 (새)대상 하드웨어 주소에 보낸다.

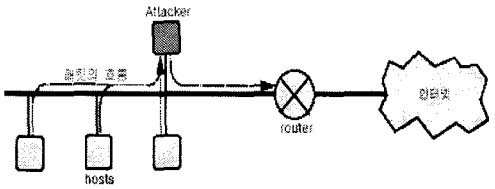
2.2 보안측면의 ARP Cache 취약성

[그림1]의 LAN상에서의 통신을 위하여 각각의 Host는 ARP cache에 송신자 프로토콜 종류, 송신자 프로토콜 주소의 체크 후(④) 두 값이 이미 cache내에 존재하면 entry의 송신자 하드웨어 주소 필드를 패킷의 새 정보로 갱신한다(⑤). 이때 공격자가 주기적으로 자신의 물리적 주소를 네트워크를 통해 ARP 패킷을 Broadcast하면 동일 LAN상의 다른 내부 Host ARP Cache에 Internet-to-Ethernet mapping 값이 공격 시스템의 값으로 변조되어 저장된다(⑤). 결과적으로 피해 시스템은 공격자 시스템을 통하여 게이트웨이로 가게 되고 공격자는 필요한 정보만을 가질 수 있다.[그림2]

또한 피해 시스템의 위조된 게이트웨이 Internet-to-Ethernet mapping값 저장과 공격자의 의도된 IP forwarding을 하지 않음으로 목적지인 게이트웨이까지 가지 못하고 인터넷에 접속이 되지 않는 DoS를 당하게 된다.[그림3]

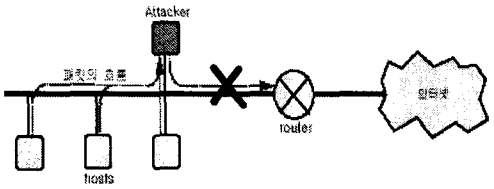
3. LAN상에서의 ARP를 이용한 공격

3.1 ARP Redirect Attack



[그림 2 - ARP Redirect Attack]

[그림 2]에서 공격자는 위조된 ARP Reply를 보내는 방법을 사용한다. 즉 공격자 Host가 위조된 ARP Reply를 Broadcast로 네트워크에 주기적으로 보내어, LAN상의 다른 모든 Host들이 공격자를 게이트웨이로 믿게 한다. 결국 외부 네트워크와 모든 트래픽은 공격자 Host를 통하여 지나가게 되고 공격자는 스니퍼를 통하여 필요한 정보를 가질 수 있게 된다.



[그림 3 - DoS Attack]

[그림 3]은 공격 시스템은 위조된 게이트웨이 물리적 주소를 LAN상의 각각의 Host에게 보냄으로써 위조된 Internet-to-Ethernet mapping값을 갖는다. 또한 공격자가 IP Forwarding을 하지 않음으로 그 결과 HOST 패킷은 게이트웨이로 가지 못하는 DoS를 일으키게 된다.

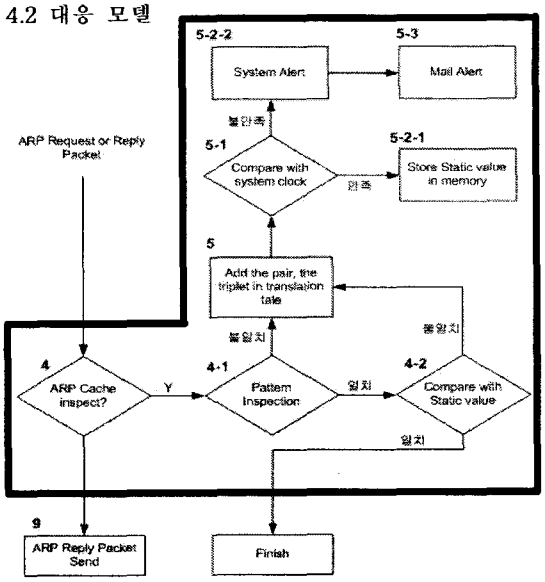
4. 대응 모델 개요와 모델

4.1 대응 모델 개요

지금까지 ARP Redirect Attack 대응 모델로서 VPN, 암호화 그리고 인증 서버를 기반으로 둔 모델들이 제안, 사용되었다. 그러나 이러한 모델들은 각각의 HOST에게 많은 비용을 부과함으로 사용되기에 어려운 단점을 지니고 있다.

본 논문에서 제안하고자 하는 Host기반의 ARP Redirect Attack에 대한 대응 모델은 비용을 들이지 않고 각각의 HOST가 LAN상에서 ARP Redirect Attack에 대한 일차 센서로서 커널에서 검사를 통하여 ARP 패킷 허용/비 허용 여부를 결정하고 HOST 스스로가 ARP 패킷 허용/비 허용을 결정하지 못할 경우 이차 센서인 최종 관리자에서 Mail Alert를 발생, 최종 관리자는 이러한 경고 수집을 통하여 일차 센서에서 결정하지 못한 패킷 허용/비 허용 유무를 판단, LAN상의 모든 일차 센서 HOST에게 통보를 해 주는 모델이다.

4.2 대응 모델



[그림 4 - ARP Redirect Attack 대응 모델]

<그림 4> 대응 모델 동작 과정

①~③ [그림1]의 ①~③까지 동작과정은 같다.

④ ARP cache에 송신자 정보를 체크한다.

④-1 일반 HOST가 게이트웨이에 접속하기 위해 APR 패킷을 LAN의 Ethernet망 또는 토큰링 망을 통해 응답자의 Reply가 올 때까지 Broadcast한다.

그러나 공격자 HOST는 ARP Redirect Attack을 행하기 위해 위조된 게이트웨이 Internet-to-Ethernet mapping값을 LAN상에 주기적으로 보내는 공격 패턴을 가지고 있다.

따라서 모든 HOST는 공격 패턴을 통한 ARP 패킷 주시검사로부터 일차 ARP 패킷/비 허용 여부를 결정한다.

④-2 패턴 검사 일치(④-1)시 HOST가 커널 변수 arp_clean_interval 과 -d를 통해 메모리에 저장된 Trusted HOST(게이트웨이) Internet-to-Ethernet mapping값 과 비교 검사 후

패킷/비 허용을 판단하는 이차 검사를 행한다.

⑤ 위 결과(④-1)가 불일치 시 공격자는 패턴을 조작하여 보낼 수 있기 때문에 일차 센서의 kernel은 패킷의 정당 유무를 위해 Internet-to-Ethernet mapping값을 다음 단계 검사를 위해 ARP cache에 임시 저장, 필드 테스트로 ARP cache를 활용한다.

⑤-1 공격 시 일반 HOST로부터 게이트웨이까지 Ping test는 공격 HOST를 거쳐야 하기 때문에 정상적인 Ping Response time과 공격 시 응답 시간과는 차이가 많이 난다.

따라서 부팅 시 커널에 의해 자동 실행되는 ping test로부터 HOST는 Trusted Host(게이트웨이)까지의 Ping Response Time 값을 가지고 있다.

그 결과로써 HOST는 두 값의 비교를 통해 패킷의 허용/비 허용 유무를 결정할 수 있다.

다음의 [표 1]의 HOST A, C는 만일 위조된 값이 들어 왔을 경우 Ping Response time은 늘어나게 되는 것을 보여 준다.

⑤-2-1 위 검사를 통하여 게이트웨이의 정당한 ARP 패킷이라 HOST 자체 판단 시 Internet-to-Ethernet mapping값을 메모리에 영구히 저장하게 된다.

HOST는 필요시 커널 변수 -d를 이용하여 entry를 제거 할 수 있다.

⑤-2-2 검사(④-1, ④-2, ⑤-1)의 검사로부터도 [표 1] HOST B와 같은 경우 HOST 자체 판단이 어려울 경우 시스템 관리자에게 Alert event를 발생시킨다

⑤-3 [표 1] HOST B와 같은 경우 위 검사를 통과하고서도 HOST 자체 판단이 어려우므로 시스템 관리자는 최종 관리자에게 Mail Alert event를 발생시킨다.

⑥~⑨ [그림 1]과 같은 동작을 한다.

Response time / Host	공격 전	공격 후	허용 오차
HOST A	0.343ms	0.653ms	± 0.1ms
HOST B	0.467ms	0.512ms	± 0.1ms
HOST C	0.298ms	0.412ms	± 0.1ms

[표 1]

5. 결론 및 향후 연구

지금까지 LAN상에서 ARP 공격 툴 들은 ARP cache의 취약점을 이용하고 있으며 피해 시스템은 자신도 모르게 정보가 노출이 되고 있는 실정이다.

본 논문에서는 LINUX 시스템 및 Windows 시스템에서 ARP Redirect Attack에 대한 ARP cache 취약성 보안 향상을 위해 ARP Cache 무 결성 검사 부분으로부터 ARP 패킷 허용/비 허용을 결정함으로써 ARP Cache의 보안을 향상하도록 하였다. 또한 공격자의 패킷 스니퍼를 거치지 않고 Host 시스템과 게이트웨이까지의 안전한 전송 및 LAN상에서 행해질 수 있는 DoS 보안을 위하여 4절과 같은 모델을 제안하였다.

Host기반 모델은 정적 네트워크 망과 비교하여 자주 환경이 변화되는 동적 네트워크 망에서의 Trusted Host 값을 저장하기에는 위에서 제시한 모델은 수시로 게이트웨이 Internet-to-Ethernet mapping값의 변화를 체크해야 하는 단점을 가지고 있다. 이를 보안할 수 있는 방법으로 HOST는 LAN상의 공격에 대해 일차 센서로서 역할을 하고 다음 보안관리를 위해 이차 센서인 Network기반 보안 모델이 고려되어야 한다.

참고 문헌

[1] RFC 826

[2] Gray R. Wright, W. Richard Stevens. TCP/IP Illustrated Volume2(2)

[3] W. Richard Stevens. UNIX Networking Programming

[4] Daniel P. Bovet & Marco Cesati. LINUX Kernel