DHCP 기반 공용 네트워크 환경에서 ARP 관련 공격 탐지 및 복구기법

김민준*, 장용준**, 신지철***, 이경현***
*부경대학교 컴퓨터공학과
**부경대학교 컴퓨터멀티미디어공학과
***부경대학교 IT융합응용공학과
*e-mail : black.cubit@gmail.com
**e-mail : wkd7881@naver.com
***e-mail : estflas@gmail.com, khrhee@pknu.ac.kr

ARP-Related Attack Detection and Recovery Technique in DHCP-based Public Networks

Min-June Kim*, Yong-Jun Jang**, Ji-Chul Shin***, Kyung-Hyune Rhee***
*Department of Computer Engineering, Pukyong National University.
**Department of Computer Multimedia Engineering, Pukyong National University.
***Department of IT Convergence and Application Engineering, Pukyong National University.

요 약

ARP 관련 공격은 LAN상에서 MAC 주소의 위조를 통해 공격대상 호스트의 패킷을 가로채어 도청이나 변조를 가능하게 하는 공격 방법 중 하나이다. 이더넷 기술의 기본이 되는 ARP 프로토콜과 이를 기본적으로 사용할 수밖에 없는 공용 네트워크의 급격한 확산은 장차 ARP 관련 공격과 그 피해가 더욱 심각해 질 것으로 예상된다. 따라서 본 논문에서는, 공용 네트워크에서 기본적으로 사용하는 DHCP 프로토콜을 이용한 ARP 관련 공격 탐지 및 복구 솔루션을 제안한다.

1. 서론

인터넷 보급이 오늘날처럼 확산되기 전에는 공용 네트워크에 대한 관심이 적었다. 하지만 휴대용 기기의 급격한 증가와 IP의 고갈에 따른 공용 네트워크의 활용이 보편화 되었다. 한편 이더넷 기술의 기본이 되는 ARP 프로토콜과 이를 기본적으로 사용할 수밖에 없는 공용 네트워크의 급격한 확산은, ARP 관련 공격의 가능성과 범위를 증대시키고 있다. ARP 관련 공격은 일반 사용자가 탐지하고 복구하는데 어려움이 크고, 네트워크 관리자들의 보안에 대한 의식 부족으로 공격에 대한 탐지 및 대책이 적절하게 이루어지고 있지 않다.[1,2] 본 논문에서는 기존 ARP 관련 공격 탐지, 방어 및 복구에 대하여 알아보고, 개선된 탐지 및 복구 기법을 제안한다.

2. 배경연구

2.1 ARP 관련 공격과 탐지

ARP 관련 공격이란, 한 네트워크 내부에서 특정 IP 주소를 갖고 있는 호스트를 찾기 위해 사용하는 ARP 테이블을 조작하여 패킷을 도청하거나 조작 할 수 있는 공격이다.[3] ARP 관련 공격방법에는 특정 호스트를 공격하는 ARP 스푸핑, 네트워크 전체를 공격하는 ARP 리다이렉트가 있다.[3]

공용 네트워크에서 ARP 관련 공격을 시도하면 일반 사용자는 속도가 약간 느려진 것을 제외하고는 변화를 알아채기 어렵다. 하지만 관련 지식이 있는 피해자는 패킷 캡처 툴을 이용하여 ARP 조작 패킷이 많이 잡히는 것을 확인하거나, ARP 테이블에 중복된 MAC 주소가 있는 것을 발견하고 공격당하고 있음을 알아챌 수 있다.

2.2 기존 ARP 관련 공격 방지대책 및 문제점

ARP 관련 공격의 방지 대책으로 첫째, 변화가 적은 네트워크에서는 ARP 테이블을 정적으로 관리하여 ARP 관련 공격을 원천 봉쇄할 수 있다.[1] 하지만 이 방법은 대규모 네트워크나 변화가 잦은 네트워크에서는 관리하기 힘들다는 단점이 있다. 따라서 게이트웨이의 IP와 MAC주소만을 정적으로 고정시킴으로써 보다 관리를 더 편리하게 할 수 있다. 하지만 이러한 방식은 모바일 네트워크 환경과 같이 IP 주소 변화가 빈번할 경우 관리가 힘들다.[3]

둘째, 개인정보나 금융정보 같이 중요한 패킷을 SSL 방식 등을 이용하여 암호화 하는 방법이다.[1] 이 방법은 인증 과정이나 키를 교환하는 과정이 공격자에게 노출될 수 있어 위험하다.

3. 제안 기법

3.1 DHCP 스캔을 이용한 ARP 관련 공격 탐지

이 장에서 초점을 두는 내용은 피해자 호스트 입장에서 자신의 ARP 테이블 내용을 갱신시키는 ARP 패킷을 수신하였을 경우 송신지 호스트가 공격자인지 공용 네트워크 게이트웨이인지 확실하게 판단하여 사용자에게 안전한 통신 환경을 제공하는 것이다.

공용 네트워크 게이트웨이와 공격자를 구분하는 방법 중 가장 일반적이면서 정확한 방법은 DHCP 프로토콜을 이용해 질의(이하 DHCP 스캔)하는 것이다. DHCP는 자동으로 IP를 분배하여 주는 기능으로 공용 네트워크 게이트웨이는 이 기능을 이용하여 제한된 고정 IP로 여러 호스트가 외부와 통신이 가능하도록 한다. 따라서 DHCP가 탑재된 라우터나 공용 네트워크 게이트웨이만 알 수 있는 DHCP 프로토콜을 이용해 질의할 경우, 그에 대한 답장은 라우터나 공용 네트워크 게이트웨이로만 보내게 된다는 것이다.[4]

만약 공격자가 DHCP 관련 공격을 함께 시도하더라도 DHCP 요청 패킷을 공용 네트워크 게이트웨이가 수신하였을 때 공용 네트워크 게이트웨이는 자신이 DHCP 서버를 가지고 있으므로 DHCP 응답 패킷을 보내주게 되고 어떤 경우라도 공용 네트워크 게이트웨이가 보낸 DHCP 응답 패킷이 먼저 도착하게 된다.

따라서 DHCP 스캔을 통해 공격자와 공용 네트워크 게이트웨이를 완벽하게 구분 가능하고 이를 이용하면 ARP 연관 공격을 완벽하게 탐지할 수 있다는 결론이 나온다. 이 결론을 바탕으로 공용 네트워크 게이트웨이 환경에서 ARP 관련 공격을 탐지하는 과정은 다음과 같다.

공격자가 공격을 시도하면 피해자 호스트의 ARP 테이블에 존재하는 게이트웨이 IP에 대한 MAC 주소는 공격자가 원하는 MAC 주소로 바뀌게 된다. 그러나 피해자 호스트는 공격에 사용된 ARP 패킷을 보낸 호스트가 공격자인지 공용 네트워크 게이트웨이인지 판단하기 어려우므로 DHCP 스캔을 수행한다. DHCP 스캔을 수행하여 돌아오는 응답을 통해 피해자 호스트는 게이트웨이의 실제 MAC 주소를 알 수 있게 되고 공격임을 판단함과 동시에 복구를 시도하거나 피해자에게 알리는 등의 추가적인 작업을 할 수 있다.

3.2 탐지 기법의 최적화

피해자 호스트가 ARP 탐지 모듈이 동작하기 위해서는 탐지할 확률만큼 중요한 것이 사용자가 불편을 느끼지 않을 만큼 시스템 자원을 적게 사용하는 것이다. 따라서 DHCP 스캔의 실행을 최소화하기 위해 다음과 같이 화이트 MAC 주소와 블랙리스트 요소를 추가로 사용한다.

- **화이트 MAC 주소**

정상적인 공용 네트워크 게이트웨이는 외부로부터 패킷이 수신될 때 내부에 대한 호스트 스캔을 수행할 수 있다. 이 경우 피해자 호스트는 ARP 조작 패킷과 같은 형태의 패킷을 수신하게 되는데 그 때마다 매번 DHCP 스캔을 수행할 경우 부하가 커진다.

- **블랙리스트**

피해자 호스트가 소속된 네트워크에서 공격자에 의한 ARP 관련 공격이 진행될 때 주기적 혹은 비주기적으로 ARP 조작 패킷이 발생한다. 이 경우 초기에는 DHCP 스캔을 통해 공격자임을 판단해야 하지만 이후에는 추가적인 DHCP 스캔이 필요하지 않다.

따라서 DHCP 스캔을 수행하여 얻은 결과를 바탕으로 화이트 MAC 주소와 블랙리스트를 설정하여 추가적인 동작을 수행하지 않도록 한다. (그림 1)은 화이트 MAC 주소와 블랙리스트를 설계하는 의사코드이다.

```
white_mac_addr = get_mac_in_arp_table(gateway_ip)
black_list = list() // data structure

while (True){
  pkt = listen(proto=arp)
  if (pkt.arp.src_mac in black_list){
    // pkt.arp.src_mac is attacker mac
    set_mac_in_arp_table(gateway_ip, white_mac_addr)
  }
  else if ((gateway_ip in pkt.arp) and (white_mac_addr is not pkt.arp.src_mac)){
    dhcp_response = dhcp_request_send(dst=broadcast)
    if (dhcp_response){
      white_mac_addr = dhcp_response.src_mac
      if (white_mac_addr is pkt.src_mac){
        // Gateway has changed.
        continue
      }
      else{
        black_list.add(pkt.src_mac)
        set_mac_in_arp_table(gateway_ip, white_mac_addr)
      }
    }
    else{
      // DHCP Server on the network does not exist.(don't care)
      continue
    }
  }
  else{
    // Packets that do not affect.(don't care)
    continue
  }
}
```

(그림 1) 화이트 MAC 주소와 블랙리스트 설계

우선 기존의 ARP 테이블에 존재하는 게이트웨이 MAC 주소를 화이트 MAC 주소로 가정한다. 그 이유는 네트워크로부터 유입되는 ARP 패킷들 중에서 조작 패킷으로 추정 가능한 패킷의 수를 줄이기 위함이다.

조작 패킷으로 추정되는 패킷의 선별은 게이트웨이 IP를 가진 ARP 패킷이 유입되었을 때, 해당 패킷에 들어있는 MAC 주소가 화이트 MAC 주소와 다를 경우에 이루어진다. 앞서 말한 선별한 패킷들은 네트워크 구성 문제로 인한 게이트웨이의 교체 일 수 있기 때문에 공격으로 판단해서는 안 된다. 따라서 위의 패킷을 보낸 호스트에 DHCP 스캔을 수행하여 돌아오는 DHCP 응답으로 조작 패킷 여부를 판단한다.

만약 DHCP 응답 패킷의 MAC 주소와 조작 패킷으로 추정하는 ARP 패킷의 MAC 주소가 일치하지 않다면 조작 패킷으로 간주하고 ARP 테이블의 게이트웨이 MAC 주소를 화이트 MAC 주소로 복구한다. 이 때 공용 네트워크 게이트웨이 환경일 경우 DHCP 응답 패킷의 MAC 주소가 게이트웨이 MAC 주소이므로 화이트 MAC 주소 값을 사전에 변경해 주어야 한다.

본 논문에서 제안하는 기법은 기존 ARP 관련 공격 탐지 기법보다 정확도 면에서는 뛰어날 수 있다 하더라도 처리 비용적인 측면에서는 비효율적일 수밖에 없다. 따라서 처리 비용을 줄이기 위해서는 호스트 기반 방화벽과의 연동이 필요하다.

3.3 호스트 기반 방화벽

DHCP 스캔의 빈도수를 줄이고 수행 성능을 향상시킬 수 있는 효과적인 방법 중 하나는 운영체제와 최적화되어 동작 가능한 호스트 기반 방화벽과의 연동이다.

호스트 기반 방화벽은 운영체제의 일부이거나 서드파티 형태로 제공되고 호스트와 관련된 모든 인/아웃바운드 트래픽을 통제하고 관리할 수 있다.[5] 따라서 최적화된 자원으로 제안하는 DHCP 스캔을 수행 가능할 것이고, 사용자가 느낄 수 있는 성능저하 문제를 최소화할 수 있다.

ARP 관련 공격은 호스트의 아웃바운드 패킷을 게이트웨이가 아닌 공격자 방향으로 바꾼다는 것을 고려할 때 호스트 기반 방화벽과의 연동은 더 효과적일 수 있다. 시스템에 ARP 테이블 변조를 탐지하는 모듈이 동작중이고 이 모듈이 변조 유무를 호스트 기반 방화벽에게 알려준다면 호스트 기반 방화벽은 아웃바운드 패킷이 감지되었을 경우에만 ARP 테이블 변조 유무를 확인한다. 만약 테이블이 변조 되었다면 DHCP 스캔을 통한 탐지 및 복구가 수행될 것이고, 그렇지 않다면 아무런 동작 없이 패킷을 포워딩한다.

4. 평가

본 논문에서 제안하는 기법은 공용 네트워크 게이트웨이 환경에서 게이트웨이를 사칭하는 ARP 관련 공격에 대한 완벽한 대처할 수 있다. 물론 이 기법을 사용할 경우 호스트의 CPU 부담이 증가할 수 있겠지만 이는 커널 기반 프록시 방화벽과의 연동을 통해 어느 정도의 비용을 줄일 수 있다.

하지만 DHCP 서버가 별도로 존재하는 라우터 환경에서 적용하기는 힘들다는 단점이 있다. 이 경우는 RIP 프로토콜을 이용할 수도 있겠지만 공용 네트워크 게이트웨이 환경에서는 기본적으로 RIP 프로토콜이 비활성화 되어서 적용이 힘들다는 점과 일반화를 위해 두 프로토콜을 동시에 사용할 경우 네트워크의 부담이 증가한다는 문제가 있다.

5. 결론

ARP 관련 공격은 일반 사용자들이 탐지하고 복구하기에는 어려움이 많다. 만약 탐지하고 복구한다고 하더라도 오탐 확률이 높고, DHCP 스캔으로 공용 네트워크 게이트웨이인지 공격자인지는 확실히 구분할 수 있기 때문에, 보다 신뢰성 있는 ARP 관련 공격 탐지가 가능하다. 제안된 방안을 최근 크게 성장하고 있는 모바일 네트워크 환경에 적용한다면 보다 신뢰성 있는 통신 보장에 도움이 될 것이다.

참고문헌

[1] KISA “TR-2007-001_ARP_Spoofing”

[2] Seungpyo Hong, Myeongjin Oh, Suyeon Lee, Sangjun Lee “Journal of KIISE” October, 2007, pp.26-30

[3] Won-Woo Choi, Jin-Wook Chung, Seong-Jin Ahn "A Study on Netw ork Security problems Analysis of ARP Mechanism" KSIAM IT series, 2004, pp.1-9

[4] Hong-il Ju, JinBum Hwang, Jong-wook Han "A study of the DHCP message authentication at home network" KIICE, 2005, pp.837-840

[5] Karen Scarfone, Paul Hoffman “Guidelines on Firewalls and Firewall Policy(Draft)” NIST, September, 2009 pp.19-20