클라우드 컴퓨팅 환경에서 가상머신의 자동화된 ARP 테이블관리를 이용한 스푸핑 방어기법 연구

강효성O 사이드울라 홍충선
경희대학교 컴퓨터공학과
{ kanghsO, saeed, cshong } @khu.ac.kr

Defense Technique against Spoofing Attacks using Automated Management of ARP Table for Virtual Machine in Cloud Computing Environment

Hyo Sung KangO Saeed Ullah Choong Seon Hong
Department of Computer Science and Engineering, Kyung Hee University

요 약

클라우드 컴퓨팅 환경에서 가상머신을 대상으로 하는 ARP Spoofing 또는 Poison이라고 불리는 네트워크 공격은 가상머신의 통신방해, 데이터 변조, 클라우드 자원 유실 등 전체 클라우드 시스템 성능저하의 원인이 되고 있다. 이를 예방하기 위해 모든 가상머신의 ARP 테이블들을 정적으로 관리하여 Spoofing 공격으로 인한 MAC 주소의 변조를 차단할 수 있지만, 클라우드 시스템 관리자가 모든 가상머신의 MAC 주소를 수작업으로 입력해야하기 때문에 대규모 클라우드 컴퓨팅 환경에서는 적용하기 어려운 한계를 가지고 있다. 이에 본 논문에서는 최근 많은 클라우드 서비스 개발 회사가 차용하고 있는 오픈소스 클라우드 플랫폼인 OpenStack 클라우드 환경에서 Spoofing 이라 불리는 네트워크 공격에 대해 자동화된 가상머신의 ARP 테이블 관리 프로세스를 통한 방어기법을 제안하고자 한다.

1. 서 론

오늘날 급격한 인터넷 활용도의 증가와 함께 인터넷이 제공하는 접근성, 편의성 등은 서버-클라이언트 중심의 기업 업무프로세스를 클라우드 환경 중심으로 바꾸었다[1]. 동시에 기업들의 클라우드 컴퓨팅 서비스를 도입과 의존도는 점점 높아져 가고 있다. 하지만 이러한 의존도는 보안적 취약함이 드러날 때 더 큰 문제를 야기할 수 있다. 미국 내 IT 컨설팅 제공업체인 가트너(Gartner)의 전세계 4개 지역, 10개국 기업들을 대상으로 한 2014년 하반기 설문조사 결과에 따르면 기업의 클라우드 서비스의 주된 도입 목적이 비용 절감, 혁신적인 업무프로세스의 실현인 것으로 나타났다. 하지만 동시에 기업들이 클라우드 도입을 망설이는 이유로 보안, 사생활 침해, 정부 감청 등에 대한 우려를 나타내고 있다[2].

그리고 이런 보안적 문제들은 클라우드 컴퓨팅 시스템을 대상으로 하는 흔히 Spoofing 또는 Poison이라고 부르는 외부 네트워크 공격으로 쉽게 구현 될 수 있다. 이런 보안적 위협요소를 예방하기 위해 모든 가상머신의 ARP 테이블들을 정적으로 관리함으로써 Spoofing 공격으로 인한 MAC 주소의 변조를 차단할 수 있지만, 클라우드 시스템 관리자가 모든 가상머신의 MAC 주소를 수작업으로 입력해야하기 때문에 대규모 클라우드 컴퓨팅 환경에서는 적용하기 어려운 한계를 가지고 있다[3].

이에 본 논문에서는 최근 많은 클라우드 서비스 개발 회사가 차용하고 있는 오픈소스 클라우드 플랫폼인 OpenStack 클라우드 환경에서 Spoofing 이라 불리는 네트워크 공격에 대해 자동화된 가상머신의 ARP 테이블 관리 프로세스를 통한 방어기법을 제안하고자 한다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-(H8501-15-1015))
*Dr. CS Hong is the corresponding author

2. 클라우드 컴퓨팅 환경에서 ARP Spoofing 공격

Address Resolution Protocol(ARP)은 네트워크 계층의 주소를 데이터 링크 계층 주소로 변환하는 표준 프로토콜로 특정 데이터를 목적지까지 전송하기 전에 목적지 IP 주소에 해당하는 MAC 주소가 ARP 테이블에 없을 경우 이를 알아내기 위해 사용한다[4]. 이런 ARP를 이용한 대표적인 네트워크 공격기법이 ARP Spoofing이다. ARP Spoofing은 공격대상자에게 조작된 ARP 응답메세지를 전달해 특정 호스트의 MAC 주소를 잘못 인식하게 하여 정상적인 통신을 방해하는 공격방식이다. 아래 그림 1은 이런 ARP Spoofing 공격 과정을 보여준다.

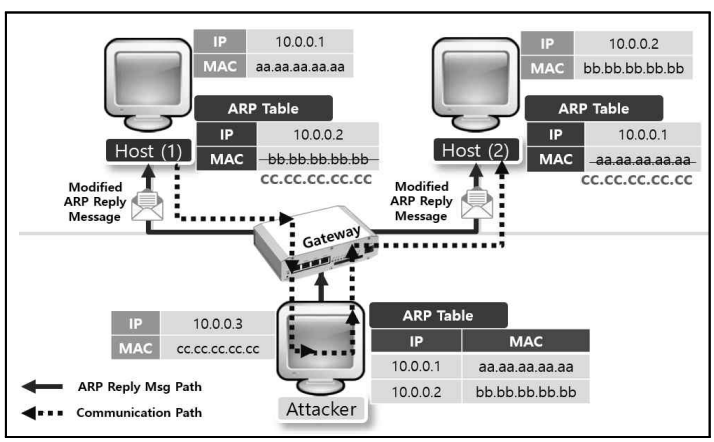

그림 1. ARP Spoofing 공격

그림 1에서 Host(1)은 Host(2)와 통신을 하기 위해 Host(2)의 MAC 주소를 알아야하며 마찬가지로 Host(2)도 Host(1)과 통신을 하기 위해 Host(1)의 MAC 주소를 알아야한다. 이를 위해 Host(1)과 Host(2)는 자신이 속해있는 서브넷에 ARP 요청메세지를 브로드캐스팅한다. 이때 같은 네트워크상에 존재하는 Attacker는 Host(1)과 Host(2)의 요청메세지를 인지하고 Host(1)과 Host(2)에 자신의 MAC 주소를 가지는 조작된 ARP 응답메세지를 보내어 Host(1)과 Host(2)의 ARP 테이블을 조작한다. 결과적으로 Host(1)은 Attacker를 Host(2)로 인식하고, Host(2)는 Attacker를 Host(1)로 인식하여 Host(1)과 Host(2)는 서로가 통신을 하고 있다고 믿지만 실제로는 Attack와 통신을 하며 정보를 Attacker에게 노출하는 결과를 낳는다. 클라우드 환경에서는 이런 ARP Spoofing 공격으로 인해 아래와 같은 문제들이 발생할 수 있다.

- 데이터 유출(Data Breaches)
- 가상머신간 통신 방해
- 데이터 변조
- 클라우드 자원 유실
- 전체 클라우드 서비스 성능 저하

특히 ARP Spoofing은 공격 대상자와 동일한 네트워크 내에서만 사용할 수 있는 공격방법이므로 대개 특별한 조치를 취하지 않고 망을 구축한다. 그러나 클라우드 환경에서는 하나의 내부 네트워크에서 여러 사용자에게 호스팅 서비스를 제공하는 환경 구성도 가능하기 때문에 Spoofing 공격을 방지하기 위한 메커니즘이 반드시 필요하다.

3. 관련 연구

3.1 정적 ARP 테이블 유지

기존 연구를 살펴보면 현재 가장 많이 상용화된 ARP Spoofing 방어기법은 가상머신의 ARP 테이블을 정적으로 유지하여 MAC 주소의 변조를 차단하는 것이다[3]. 하지만 이 경우 클라우드 시스템 관리자가 모든 가상머신의 MAC 주소를 수작업으로 입력해야하기 때문에 대규모 클라우드 컴퓨팅 환경에서는 적용하기 어려운 한계를 가지고 있다.

4. 제안 사항

본 논문에서 클라우드 환경은 오픈소스 클라우드 플랫폼인 OpenStack에서 가상머신의 생성 및 관리를 담당하는 Compute Node 내부에서 구현된다[5]. 그리고 제안하는 방어기법은 생성된 가상머신들의 MAC 주소정보를 수집하는 Controller Agent 부분과 ARP 테이블을 자동으로 갱신해주기 위하여 Controller Agent로부터 OpenStack 내부 가상머신의 MAC 주소정보를 수신받는 VM Agent로 구성된다. 아래 그림 2는 본 논문에서 제안하는 자동화된 가상머신의 ARP 테이블 관리 프로세스를 보여준다.

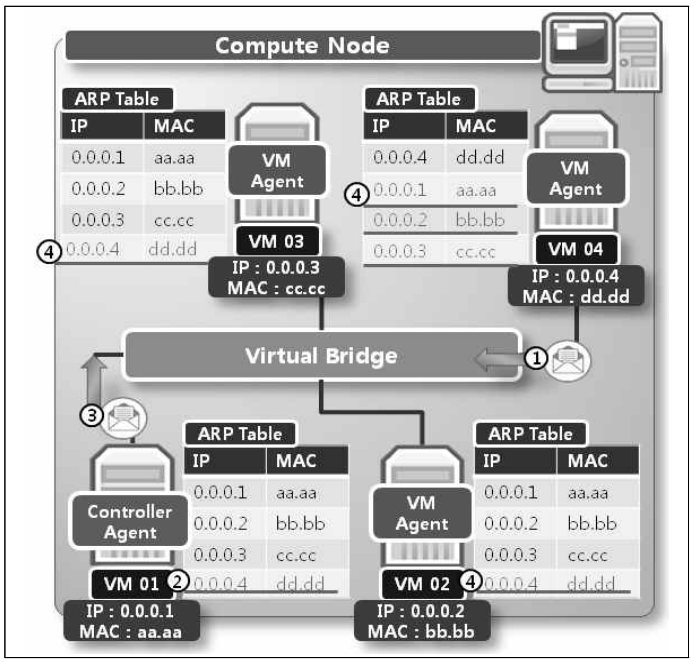

그림 2. 자동화된 ARP 테이블 관리 프로세스

우선 그림 2에서 Compute Node 내부의 가상머신 VM 01에는 Controller Agent를 관리자가 직접 구성한다. 그리고 그 외 가상머신들은 처음 생성될 때 자동으로 VM Agent가 구성되도록 설정한다. 현재 그림 2에서 가상머신 VM 01, VM 02 그리고 VM 03의 ARP 테이블에는 서로의 IP, MAC 주소 정보를 가지고 있기 때문에 서로 통신을 할 수 있는 상태이며 여기에 새로운 가상머신 VM 04를 생성했을 때의 세부 시나리오는 아래와 같다.

① 가상머신 VM 04가 생성되면 VM 04의 VM Agent는 생성된 가상머신의 MAC 주소정보를 Controller Agent에 암호화하여 전송한다.
② Controller Agent는 수신받은 VM 04의 MAC 주소정보를 가지고 자신의 ARP 테이블을 갱신한다.
③ Controller Agent는 새로 생성된 VM 04의 VM Agent에는 지금까지 구축된 모든 가상머신들의 MAC 주소정보를 암호화하여 보내고, 기존에 생성되어 있는 가상머신 VM 02, VM 03의 VM Agent에는 새로 생성된 VM 04의 MAC 주소정보를 암호화 하여 보낸다.
④ VM Agent는 수신받은 MAC 주소정보를 가지고 ARP 테이블을 갱신함으로써 모든 가상머신들의 ARP 테이블이 똑같은 MAC 정보를 자동으로 유지하게 된다.

여기서 클라우드 내부 모든 가상머신들의 VM Agent들은 Controller Agent와의 보안적 채널을 통해서 ARP 테이블을 자동으로 유지하기 때문에 ARP 프로토콜을 통한 응답메세지를 받을 필요가 없다. 즉, Agent 사이의 채널을 통한 메시지 송수신 외에는 모두 차단함으로써 ARP Spoofing 공격을 원천적으로 차단 할 수 있다.

5. 성능분석

성능분석을 위하여 클라우드 외부 호스트에서 실제 163.180.116.21의 IP를 가지는 가상머신에 대해 ARP Spoofing 공격을 시도한다[6]. 그리고 해당 가상머신 ARP 테이블의 변조 여부를 판단하여 성능평가를 진행하였다.

```
Interface: 163.180.116.21 --- 0x3
 Internet Address      Physical Address    Type
 163.180.116.26        50-46-5d-73-3f-bf   dynamic
 163.180.116.27        d0-50-99-12-84-fc   dynamic
 163.180.116.28        00-e0-4c-36-e6-7d   dynamic
```

그림 3. Spoofing 공격 전 가상머신의 ARP 테이블

```
Interface: 163.180.116.21 --- 0x3
 Internet Address      Physical Address    Type
 163.180.116.26        50-46-5d-73-3f-bf   dynamic
 163.180.116.27        c4-7d-4f-73-a6-7f   dynamic
 163.180.116.28        00-e0-4c-36-e6-7d   dynamic
```

그림 4. Spoofing 공격 후 가상머신의 ARP 테이블

```
Interface: 163.180.116.21 --- 0x3
 Internet Address      Physical Address    Type
 163.180.116.26        50-46-5d-73-3f-bf   dynamic
 163.180.116.27        d0-50-99-12-84-fc   dynamic
 163.180.116.28        00-e0-4c-36-e6-7d   dynamic
```

그림 5. 방어기법 적용 후 가상머신의 ARP 테이블

그림 3은 Spoofing 공격 전 가상머신의 ARP 테이블이다. 현재 163.180.116.21 IP를 가지는 가상머신의 ARP 테이블에는 163.180.116.26~28 3개의 IP에 대한 MAC 주소 정보를 가진 것을 확인 할 수 있다. 그림 4는 Spoofing 공격 후 가상머신의 ARP 테이블이다. 그림 3과 달리 163.180.116.27의 MAC 주소 정보가 공격자의 MAC 주소정보로 변조된 것을 확인 할 수 있다. 그림 5는 제안된 방어기법이 적용된 후 ARP Spoofing 공격을 시도한 가상머신의 ARP 테이블이다. Spoofing 공격이 모두 차단되어 그림 3과 같이 Spoofing 공격 전의 ARP 테이블을 유지하는 것을 확인할 수 있다.

6. 결론

본 논문에서 제안된 기법은 자동으로 가상머신의 ARP 테이블을 유지하기 때문에 외부에 추가적인 장비나 구성이 필요없으며 대규모 클라우드 환경에 적용하기도 용이하다. 또한 Controller Agent와 VM Agent 사이의 보안 채널을 통해 ARP 테이블을 유지하므로 ARP 프로토콜을 통한 ARP 요청, 응답메세지를 직접 송수신할 필요가 없다. 즉, 원천적인 Spoofing 공격 차단이 가능하다. 하지만 Controller Agent가 관리하는 가상머신의 ARP 테이블을 기준으로 모든 가상머신의 ARP 테이블을 유지하기 때문에 Controller Agent가 공격자에게 노출될 경우 전체 가상머신에 대한 정보가 노출 될 수 있는 한계점도 가지고 있다. 하지만 앞으로 조금만 더 개선된다면 실제 클라우드 컴퓨팅 환경에 적용 할 수 있을 것이라고 전망한다.

참고문헌

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

[2] Gartner, "전세계 클라우드 도입현황", 2014. 12.

[3] V. Ramachandran and S. Nandi, "Detecting ARP spoofing: An active technique," Lecture Notes in Computer Science, vol.3803, pp.239-250, 2005.

[4] Issac, Biju. "Secure ARP and secure DHCP protocols to mitigate security attacks." arXiv preprint arXiv:1410.4398 (2014).

[5] Rasib Hassan Khan, Jukka Ylitalo, Abu Shohel Ahmed, "OpenID authentication as a service in OpenStack", 2011 7th Information Assurance and Security (IAS), pp.372-377, 2011. 12.

[6] Cain & Abel, http://www.oxid.it/projects.html