클라우드 시스템에서 브릿지 통합 및 플로우 기반 패킷 필터를 이용한 ARP spoofing 공격을 방어하는 방법

임재민, 김영필, 유혁*

*고려대학교 정보대학

A method for defending cloud system against ARP spoofing attacks using bridge integration and flow-based packet filter

Jea-Min Lim, Young-Pil Kim, Chuck Yoo*

*College of Informatics, Korea University.

요 약

클라우드 컴퓨팅은 저렴한 유지비용으로 인해 많은 기업에서 도입하고 있지만, 복잡한 클라우드 환경의 특성상 ARP(Address Resolution Protocol) 스푸핑(spoofing) 같이 간단한 공격이더라도 탐지가 쉽지 않고, 보안 사고가 발생했을 때 내부 정보 유출 가능성이 높다. 따라서 본 논문에서는 클라우드 환경에서 브릿지(bridge)를 통합하고, 통합 된 브릿지에서 패킷 필터를 이용하여 ARP 스푸핑을 막는 기법을 제안한다. 그리고 이 기법을 통해 클라우드 내부에서 발생되는 ARP 스푸핑을 막을 수 있음을 보여준다.

Keyworks: Cloud computing, ARP spoofing, network security

I. 서론

최근 주목 받고 있는 클라우드 컴퓨팅은 낮은 초기 도입 비용과 사용한 만큼 비용을 지불하는 정책으로 인해 보급이 증가하고 있다. 하지만 클라우드 환경에서 발생할 수 있는 보안 사고에 대한 우려의 목소리가 커지고 있다.

표 1은 클라우드 환경에서 발생하는 보안 위협을 분류한 표이다. 이 중 계정 또는 서비스 강탈(Account or Service hijacking), 데이터 유출(Data leakage), DoS(Denial of Service) 같은 보안 위협은 클라우드 내부 네트워크의 보안 취약점에 의해 발생 될 수 있다. 클라우드 환경의 특성상 네트워크 구조가 복잡하여 스니핑(sniffing)이나 스푸핑(spoofing)같이 내부에서 발생되는 공격에 대해 탐지가 어렵고 막는 방법을 적용하는 것이 쉽지 않다. 기존 연구에서는 보안을 고려한 새로운 ARP(Address Resolution Protocol) 프로토콜(protocol)[2]을 제안하였고, 네트워크 구조를 개선[3] 하는 등의 연구가 진행 되어왔지만 기존에 클라우드 환경을 대체해야한다는 한계점을 가지고 있다.

No	Threats
1	Account or service hijacking
2	Data scavenger
3	Data leakage
4	Denial of Service
5	Customer-data manipulation
6	Virtual machine escape
7	Virtual machine hopping
8	Malicious virtual machine creation
9	Insecure virtual machine migration
10	Sniffing/Spoofing virtual network

표 1. 클라우드 환경의 보안 위협[1]

※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.R0126-15-1066,(SW 스타랩) 성능 및 보안 SLA 보장이 가능한 차세대 클라우드 인프라SW 개발)

※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.B0126-15-1046,SDN 2.0 실현을 위한 네트워크 가상화 플랫폼 핵심 기술 및 서비스 연구)

본 논문에서는 OpenStack 클라우드 플랫폼에서 플렛폼 수정을 최소화 하면서 ARP 스푸핑을 막을 수 있는 플로우(flow) 기반의 패킷 필터 방법과 패킷 검사를 강제할 수 있는 소프트웨어 스위치(software switch)기반의 네트워크 프레임워크를 제안한다.

II. ARP의 보안 취약점

ARP 스푸핑은 ARP의 취약점을 악용한 공격 방법으로 피해자의 데이터를 유출해 보안 사고를 유발 시킬 수 있다. ARP는 네트워크 계층의 주소인 IP(Internet Protocol)과 데이터 링크 계층의 주소인 MAC(Media Access Control Protocol) 주소를 연결시킬 때 사용하는 프로토콜로 패킷을 목적지로 전달하기 위해 다음 홉의 MAC 주소를 요청할 때 사용된다. 이 프로토콜의 보안 취약점은 호스트를 검증하지 않는 점이다. 이것을 악용할 경우 ARP 스푸핑이 가능하다. 이 공격은 공격자가 피해자에게 변조된 ARP 응답을 보내 피해자가 패킷을 공격자에게 전송하도록 하는 방법으로 패킷에 담겨있는 정보 유출 같은 보안 사고를 일으킬 수 있다.

III. 관련 연구

앞에서 설명한 ARP의 취약점을 막기 위한 방법으로 다양한 기법이 제시 되었다. 한 연구에서는 ARP를 확장하여 인증 개념을 추가한 S-ARP를 제안 하였고, 또 다른 연구에서는 가상 네트워크 프레임워크를 제안하였다. 마지막으로 OpenStack 환경에서 ARP 메시지(message) 검증을 위해 인증서비스를 제공하는 Keystone을 이용하는 기법이 제안되었다.

2.1 인증이 추가 된 ARP: S-ARP[2]

S-ARP(Secure Address Resolution Protocol)는 기존 ARP 메시지를 인증할 수 있도록 확장한 새로운 프로토콜이다. S-ARP는 기존 ARP와 다르게 DSA(Digital Signature Algorithm)을 이용한 메시지 인증 기능이 있다. 이 프로토콜을 통해 ARP 메시지의 변조를 막을 수 있지만, 키 관리 비용이 추가되고, ARP 요청 및 응답 메시지의 길이가 증가한다. 그리고 모든 시스템을 S-ARP가 동작하도록 교체해야하는 문제가 있다.

2.2 Xen 기반 가상 네트워크 프레임워크[4]

이 연구는 Xen 기반의 가상화 환경에서 수평적(flat)인 TCP/IP 네트워크를 라우팅 계층, 방화벽 계층 그리고 공유 계층으로 나누는 가상 네트워크 프레임워크를 제시하고 있다. 이 프레임워크에서는 스니핑 또는 스푸핑 공격이 발생하더라도 내, 외부와 연결되는 트래픽이 방화벽 계층을 거치기 때문에 공격 탐지 및 방어가 가능한 장점이 있다. 하지만 공유 계층 내부 통신에 대한 공격 탐지 및 방어가 불가능하다.

2.3 Keystone기반의 ARP 메시지 인증[4]

Keystone은 OpenStack 클라우드 환경에서 사용자를 인증해 주는 서비스를 제공한다. 이 서비스를 이용하여 가상 머신의 IP/MAC 주소를 저장한 인증 테이블을 구성하고, 클라우드 내부에서 발생 된 ARP 메시지와 인증 테이블을 비교하여 변조 된 메시지인지 검증한다. 하지만 ARP 패킷을 전수 검사를 위해 Keystone이 설치된 물리 머신에 전달해야 한다는 점 때문에 트래픽이 증가하고, 인증 테이블을 관리해야하는 비용이 추가 된다.

IV. 제안하는 방법

본 논문에서는 클라우드 환경을 고려하여 ARP 스푸핑 공격을 막을 수 있는 방법으로서 첫째, 소프트웨어 스위치를 이용한 가상 브릿지(virtual bridge)통합과 둘째, 플로우 기반의 패킷 필터를 이용한 가상 네트워크 프레임워크를 제안한다. 클라우드 환경에서는 가상 머신이 가상 브릿지를 공유하도록 구성되어 있어 보안 관점에서 볼 때 스니핑 또는 스푸핑 같은 공격에 취약하다[1][4]. 하지만 이것을 해결하기 위해 가상 브릿지를 가상 머신마다 독립적으로 구성하는 방법은 현실적으로 불가능하다. 따라서 공유되는 가상 브릿지의 개수를 최소한으로 줄이고 가상 브릿지에서 패킷 필터를 통해 공격을 차단하는 기법을 본 논문에서 제안 한다.

3.1 통합된 브릿지의 구성 방법

클라우드 환경에서 가상 머신 간 공유되는 브릿지의 숫자를 최소한으로 줄이기 위해 본 논문에서는 소프트웨어 스위치를 기반으로 그림 1과 같이 통합된 브릿지를 구성 한다.

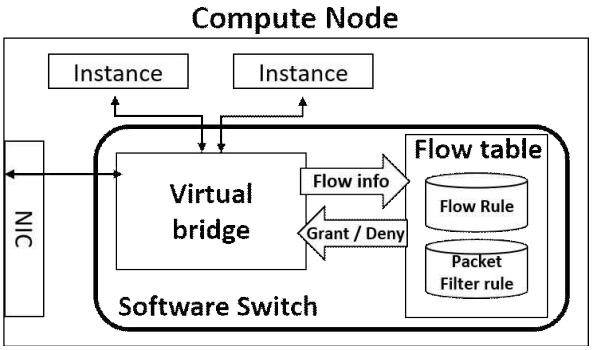

그림 1. 소프트웨어 스위치 기반의 통합된 경로

기존 가상 브릿지는 단순한 L2 스위칭을 제공한다. 따라서 다양한 가상 네트워크 프로토콜 지원 이나 QoS(Quality of Service) 같은 상위 계층의 기능을 제공하기 힘들고, 많은 수의 가상 네트워크를 구성하기 위해서는 브릿지의 개수가 늘어나 관리가 힘들어진다. 하지만 이것을 소프트웨어 스위치를 사용할 경우 다양한 계층에서 제공하는 기능을 사용할 수 있고, 통합 관리가 가능하다. 그림 1은 본 논문에서 제안하는 통합된 경로를 보여주는 그림으로 가상 브릿지와 플로우 테이블로 구성 되어 있다. 가상 브릿지는 가상 머신의 네트워크 인터페이스와 물리 머신의 네트워크 인터페이스와 연결하는 역할을 한다. 가상 브릿지를 통과하는 패킷은 플로우 테이블에 정의된 패킷 처리 정책에 따라 버려지거나 가상머신 또는 외부로 전송 된다. 경로 통합 방법을 통해 공유 되는 가상 브릿지의 숫자를 최소한으로 구성할 수 있다.

3.2 플로우 기반의 패킷 필터

본 논문에서 ARP 스푸핑을 막기 위한 패킷 필터 방법(packet filer)은 플로우 기반의 정책을 플로우 테이블에 정의하여 ARP 메시지가 유효한지 검사한다. 플로우 기반 패킷 처리 방법이 가지는 장점은 OpenFlow[6] 장비와 호환성을 가진다는 것과. 복잡하고 빠르게 변하는 클라우드 네트워크의 특성상 다양한 프로토콜

Packet Filter rule (table 0)

No	src MAC	dst MAC	src IP	dst IP	Protocol	Action
0	VM MAC	.	VM IP	.	ARP	normal
1	.	.	.	.	ARP	drop
2	.	.	.	.	.	Resubmit (table1)

Flow rule (table1)

No	src MAC	dst MAC	src IP	dst IP	Protocol	Action
0	.	.	.	.	.	normal

그림 2. 패킷 필터를 위한 플로우 정책 구성

에 대한 처리 정책을 설정할 수 있어 확장성이 좋고, 플로우에 대한 통계를 수집하여 관리자는 네트워크 상태를 비로 확인할 수 있는 장점이 있다. 그림 2는 패킷 필터을 고려한 플로우 테이블의 구성을 나타낸 그림이다. 기존에 있던 플로우 테이블 앞에 패킷 필터를 위한 플로우 테이블을 추가하여 플로우 테이블의 수정 없이 패킷 필터 기능을 추가로 사용할 수 있다. 그림 2에서 보이는 정책은 ARP 공격을 막을 수 있는 정책의 예로 가상 머신의 IP 주소와 MAC 주소를 등록한 모습이다.

3.3 공격 시나리오와 대응 방안

이 장에서는 클라우드 내에서 발생하는 ARP 스푸핑 시나리오를 보이고, 제안하는 기법을 통해 공격이 무력화 되는 것을 보인다.

- 공격 시나리오

공격자(Attacker)의 가상 머신은 피해자(Victim)의 가상 머신과 같은 클라우드에 동일한 물리 머신에서 동작하는 상황에서 피해자에게 전송 될 패킷을 가로채기 위해 ARP 스푸핑을 하려고 한다. 공격자와 피해자의 가상머신 및 가상 브릿지의 IP 와 MAC 주소는 표 2 와 같이 구성 되어 있다고 가정한다.

Name	IP address	MAC address
Virtual Bridge	10.0.0.1	0c:xx:xx:xx:xx:01
Victim	10.0.0.2	fa:xx:xx:xx:xx:01
Attacker	10.0.0.3	fa:xx:xx:xx:xx:02

표 2. 공격 시나리오 상의 IP와 MAC 주소

클라우드 외부에서 들어온 패킷의 경로를 알기 위해 가상 브릿지는 피해자의 IP 주소인

10.0.0.2 의 MAC 주소를 10.0.0.1 에게 알려 달라는 ARP 요청을 브로드캐스트(broadcast) 한다. ARP 요청 메시지를 받은 공격자는 ARP 스푸핑을 하기 위해 ARP 응답 메시지를 변조 한다. 공격자는 정상적인 ARP 응답 메시지 대신 자기가 패킷을 받을 수 있도록 10.0.0.1 에게 10.0.0.2 의 MAC 주소가 fa:xx:xx:xx:xx:02 라는 응답을 유니캐스트(unicast) 한다. 변조 된 메시지를 받은 가상 브릿지는 ARP 테이블의 정보를 10.0.0.2 - fa:xx:xx:xx:xx:02 과 같이 기록하여 ARP 스푸핑이 성공 한다.

- ARP 스푸핑에 대한 대응 방법

앞에서 언급한 시나리와 동일한 환경에서 사전에 관리자는 제안하는 기법을 적용했을 때 대응 하는 방법을 설명한다. 패킷 필터에 등록 될 보안 정책은 표 3 과 같이 등록하여 ARP 패킷에 대해 IP와 MAC 주소가 맞는지를 검사하고 만약 IP와 MAC 주소 쌍이 틀릴 경우 버리도록 구성 한다.

No	IP	MAC	proto	Action
0	10.0.0.1	0c:xx:xx:xx:xx:01	ARP	normal
1	10.0.0.2	fa:xx:xx:xx:xx:01	ARP	normal
2	10.0.0.3	fa:xx:xx:xx:xx:02	ARP	normal
3	*	*	ARP	drop

표 3. ARP 공격을 막는 패킷 필터 정책

공격자로부터 출발한 변조된 ARP 응답은 가상 브릿지의 패킷 필터를 거친다. 이 변조된 응답은 IP와 MAC 주소가 각각 10.0.0.2 과 fa:xx:xx:xx:xx:02 이기 때문에 표 3의 3번 정책에 의해 패킷이 버려지게 된다.

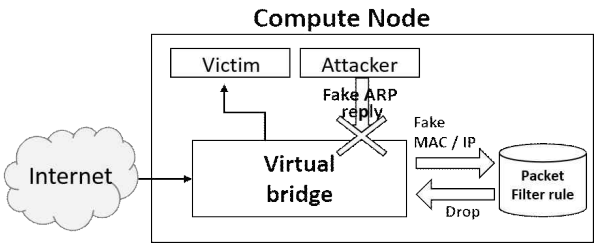

그림 3. ARP 스푸핑에 대한 대응 방식

따라서 변조된 ARP 응답에 의해 가상 브릿지의 ARP 테이블은 업데이트가 일어나지 않게 되어 공격자가 시도한 ARP 스푸핑 공격이 무력화됨을 확인 할 수 있다.

V. 결론

본 논문에서는 클라우드 시스템 내부에서 발생되는 ARP 스푸핑을 막을 수 있는 통합 된 브릿지 및 필터 정책을 제안하였다. 통합 된 경로 상에서 플로우 테이블 기반의 정책 구성을 통해 다양한 프로토콜에 대한 확장성과 관리의 편리성을 가지고 있다. 본 논문의 한계점은 클라우드 내부에서 발생 되는 공격만을 가정하고 있기 때문에 외부에서 발생되는 공격에는 검증이 필요하고, 가상 네트워크 프로토콜을 고려하고 있지 않다. 추후 제안한 구조를 토대로 실제 시스템을 구축하고 가상 네트워크 프로토콜을 지원하도록 할 예정이다.

[참고문헌]

[1] K Hashizume et al., An analysis of security issues for cloud computing, Journal of Internet Services and Applications, a Springer open journal, February, 2013

[2] G. Gouda and H. Chin-Tser, A Secure Address Resolution Protocol, Computer Networks, vol.1, no.41, January, 2003.

[3] H. Wu, Y. Ding, L. Yao, and C. Winer, Network security for virtual machine in cloud computing, Int Conf on Computer Sciences and Convergence Information Technology, Nov. 30-Dec. 2, 2010.

[4] 강효성, 홍충선, OpenStack 클라우드 컴퓨팅 환경에서 Keystone 인증 서비스를 이용한 ARP Spoofing 방어기법, 한국정보과학회 학술발표논문집, June, 2015.

[5] D. Nurmi, et al. The eucalyptus open-source cloud-computing system. Cluster Computing and the Grid, May, 2009

[6] N.McKeown et al., OpenFlow: enabling innovation in campus networks, ACM SIGCOMM Computer Communication Review, April, 2008