IP Spoofing을 이용한 분산 반사 서비스 거부 공격의 보안 위협과 대응 실태 연구

홍윤석[1] · 한우영[2*]

[1]고양일고등학교 · [2]한국디지털미디어고등학교

A Study of security threats and response of Distribute Reflection Denial of Service Attack using IP spoofing

YunSeok, Hong[1] · Wooyoung Han[2*]

[1]Goyang il High School

[2]Korea Digital Media High School

E-mail : me@yunseok.kr / hanu@dimigo.hs.kr

요 약

전 세계적인 인터넷의 보급으로 인터넷과 연결된 기기들이 점차 늘어나고 있다. 이에 더불어 DNS, NTP, CLDAP 와 같이 응용 프로토콜의 취약점을 이용하여, 공격자가 피해자인 것처럼 아이피를 속여, 다량의 응답을 악의적으로 요청하는 공격인 분산 반사 서비스 거부 공격(DRDoS)이 급격하게 늘어나는 추세이다. ISP 들이 IP Spoofing에 대한 적절한 대비책을 수립하지 않으면 분산 반사 서비스 공격의 보안 위협은 사라지기 어려울 것으로 사료된다. 따라서 본 논문에서는 IP Spoofing에 기반한 분산 반사 서비스 공격의 보안 위협과 대응 실태에 관해 기술한다.

ABSTRACT

With the spread of the Internet around the world, devices connected to the Internet are gradually increasing. In addition, the number of distributed reflection service attacks (DrDoS), an attack that maliciously requests large responses by deceiving IPs as if the attacker was a victim, using vulnerabilities in application protocols such as DNS, NTP, and CLDAP, is increasing rapidly. It is believed that the security threat of distributed reflection service attacks will not disappear unless ISPs establish appropriate countermeasures to IP Spoofing. Therefore, this paper describes the security threat and response status of distributed reflection service attacks based on IP Spoofing.

키워드

IP Spoofing, DrDoS, Autonomous Systems, 분산서비스거부공격

Ⅰ. 서 론

본 논문에서는 전 세계적인 인터넷 보급으로 인터넷과 연결된 기기들이 점차 늘어남에 따라 다양한 목적을 가진 DNS, NTP, CLDAP 서비스도 증가하는 추세이다. 이러한 서비스가 운영되는 장비 중에도 치명적인 네트워크 취약점인 IP Spoofing이 가능한 ISP에 연결된 장비가 존재하여, 피해자의 IP를 스푸핑해 공격자가 다량의 응답이 피해자에게 가도록 악의적으로 외부 서버에 요청하는 공격인 분산 반사 서비스 공격(DRDoS)가 늘어나고 있다. 또한 이런 공격을 금전을 받고 대행해 주는 서비스들도 존재하여 잠재적으로는 DDoS 공격보다 더욱 큰 파장을 일으킬 수 있을것으로 예상된다. 국내 특정 ISP에서 IP Spoofing 공격이 가능함에 따라 분산 반사 서비스 공격이 어떤 보안 위협을 주는지, 그리고 실제 국내 및 전세계 ISP의 IP Spoofing 대응 실태에 대해 저술하고자 한다.

Ⅱ. IP Spoofing

IP Spoofing은 인터넷 프로토콜(Internet Protocol, IP) 패킷의 앞부분에 있는 헤더에서 패

* speaker

킷을 보낼 때 자신의 IP 주소를 뜻하는 송신지 주소(Source Address)를 위조하는 공격 기법을 의미한다.

일반적인 경우 IP Spoofing 공격은 Bogon-list를 사용한 필터링 정책이나 uRPF(unicast Reverse Path Forwarding), 스위치에서 IP Source Guard를 통해 차단되어 있으나, 일부 ISP의 경우 해당 조치를 하지 않아 IP 스푸핑이 가능한 경우가 있다.

최근 제로트러스트 보안정책을 펼치는 기업 내부망이나 업무망의 경우 아이피를 기반으로 서비스의 접근을 필터링 하는 경우가 많아 IP를 스푸핑을 통해 접근이 제한된 서버에 접근하는데 악용될 수 있는 위험성이 높은 네트워크 취약점이라고 볼 수 있다.

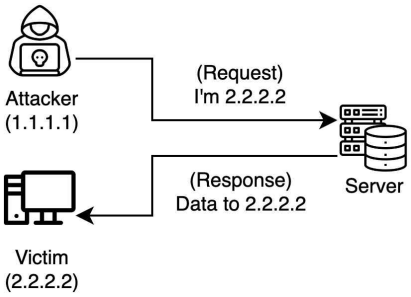

그림1. IP Spoofing 공격 과정

Ⅲ. 분산 반사 서비스 거부 공격(DRDoS)

분산 반사 서비스 거부 공격은 피해자의 IP를 스푸핑하여 운영 중인 DNS, NTP, CLDAP와 같은 서비스 서버에 피해자의 아이피로 다량의 응답을 하도록 악의적으로 요청하는 것을 의미한다.

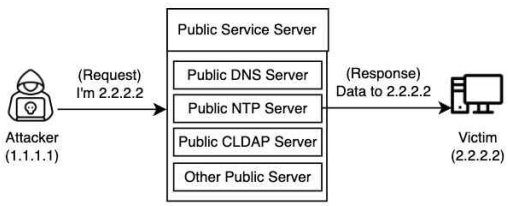

그림2. 분산 반사 서비스 거부 공격(DRDoS) 과정

공격자가 분산 반사 서비스 거부 공격을 하기 위해서는 IP 스푸핑이 가능한 인터넷 회선을 준비하고 반사체로 사용될 서버를 선정한 뒤, 피해자의 아이피로 스푸핑하여 해당 서버에 요청을 보내 다량의 응답을 하도록 유도하여 공격을 할 수 있다.

분산 반사 서비스 거부 공격이 위험한 이유는 반사체 공격의 특성상 공격자가 서버로 보낸 요청보다 수천배 이상의 응답을 피해자가 받도록 할 수 있기 때문이다. 이러한 점을 악용하면 DDoS 공격에 비해 규모가 훨씬 큰 수Tbps 급의 공격이 될 수 있다. 최근 공개된 Memcached UDP 취약점에 기반한 DRDoS의 경우 5만배 이상의 증폭이 가능하여 일반적인 가정에 들어가는 1Gbps 회선을 기준으로 보았을 때 이론상으로는 50Tbps 이상의 공격이 가능하다고 볼 수 있다.

Ⅳ. 분산 반사 서비스 거부 공격으로 인한 보안 위협

전세계 공격자들의 서비스 거부 공격을 대비하기 위해서 여러 상용 디도스 방어 서비스 제공 업체들은 Anycast 라우팅 방식과 ECMP(Equal Cost Multi-path) 라우팅 방식을 사용해 국제망으로 공격을 분산해 완화하여 공격을 방어하고 있다.

하지만 국제망 기반 공격 완화 방식은 서비스 규모가 커질수록 구축이 복잡하고 비용이 높아져 모든 서비스들이 국제망으로 공격을 분산해 완화시키는 라우팅 기법을 사용할 수 없고, 모든 서비스를 폐쇄적인 환경에서만 운영 할수도 없기 때문에 분산 반사 서비스 거부 공격은 인터넷의 근간을 위협하는 큰 문제라고 볼 수 있다.

분산 반사 서비스 거부 공격의 반사체로 쓰이는 어플리케이션들은 실시간성을 요구하는 어플리케이션들이 많아 UDP를 사용한다는 공통점이 있다. 분산 반사 서비스 거부 공격을 방어하기 위해서 백본에서 UDP 프로토콜을 차단하게 될 경우, 다른 서비스들이 정상적으로 작동하지 않을 가능성이 높아 완벽한 해결책이라 보기 어렵다.

그러나 NTP 서버의 경우 공격이 올 때 페이로드를 참조하여, 공격을 방어할 수 있으며, DNS 서버의 경우 내부적으로 DNS Relay 서버를 구축하여 차단하고 운영하는 방법이 존재하는 등 각 프로토콜에 특징에 기반하여 분산 반사 서비스 거부 공격을 방어하는 방법이 활발하게 연구되고 있다.

Ⅴ. 국내 통신사 및 국외 통신사 대응 실태

캘리포니아 대학교 샌디에이고 슈퍼컴퓨터 센터에 기반을 둔 네트워크 관련 연구기관인 CAIDA에서 발표한 내용[1]에 따르면 대한민국 회선은 작년 기준 전체 테스트 결과 중 5.3%가 IP Spoofing이

가능한 것으로 보고되었다.

예상보다 너무 많은 국내 회선이 IP 스푸핑이 가능하다는 결과가 나와 이를 검증하기 위해 직접 국내 3사 ISP K사, L사, S사의 가정용 회선과 기업용 회선을 직접 준비하여 CAIDA에서 배포하는 <Spoofer>를 사용해 IP 스푸핑 결과를 확인 해 보았다.

표 1. 국내 통신사 대응 실태

	K사	L사	S사
가정용 회선	X	X	X
기업용 회선	X	O	X

실제로 L사 기업용 회선에서 IP 스푸핑이 가능하다는 것을 확인할 수 있었고, 해당 내용을 ISP와 관련 정부 부처에 공유하여 현재는 IP 스푸핑에 대한 차단 정책을 수립하고 개선이 된 상태이다. 개선 이후 CAIDA의 리포트를 다시 확인하였을 때 4.7%의 국내 회선이 IP 스푸핑에 취약한 것으로 확인 되었고, 국내 취약 회선중 L사 기업용 회선이 0.6%를 차지하고 있음을 확인할 수 있었다.

국외 통신사중에서도 브라질, 인도, 미국, 이집트, 아르헨티나 등 다양한 국가에서 현재까지도 IP 스푸핑이 가능함을 CAIDA의 리포트를 통해 확인할 수 있었다.

Ⅵ. 결 론

인터넷 기술은 비약적으로 발전하고 있음에도 불구하고 기본적인 네트워크 취약점인 IP 스푸핑 공격에 대한 보안 조치가 되지 않은 경우가 국내 대표 3사 ISP중에도 있음을 확인 할 수 있었다. CAIDA 리포트에 따르면 전 세계 IPv4 대역 중 21%가 IP 스푸핑에 취약하고, IP Spoofing 공격을 활용한 분산 반사 서비스 공격이 계속해서 이뤄지고 있으며 다양한 어플리케이션을 반사체로 공격을 증폭하는 패턴을 보이기 때문에 다른 공격에 비해 대응하기 어려워지고 있다. ISP의 인터넷 보안 기술에 대한 관심과 대응을 통해 IP 스푸핑이 원천적으로 차단되어 인터넷이 더욱 안전해지길 바라며 본 논문을 마친다.

References

[1] Center for Applied Internet Data Analysis. State of IP Spoofing [Internet]. Available : https://spoofer.caida.org/summary.php

[2] S. Shaw and P. Choudhury, "A new local area network attack through IP and MAC address spoofing," *2015 International Conference on Advances in Computer Engineering and Applications*, 2015, pp. 347-350, doi: 10.1109/ICACEA.2015.7164728.

[3] Y.Hong, W.Han. A Study on Efficient DDoS Protection Techniques using Anycast and BGP ECMP. The Korea Institute of Information and Communication Engineering, 2022, 26 (1), 125-128.

[4] H. Lema, F. Simba and A. Ally, "Preventing Utilization of Shared Network Resources by Detecting IP Spoofing Attacks through Validation of source IP Address," IST-Africa Week Conference (IST-Africa), 2018, pp. 8-8.

[5] C. Manusankar, S. Karthik and T. Rajendran, "Intrusion Detection System with packet filtering for IP Spoofing," 2010 International Conference on Communication and Computational Intelligence (INCOCCI), 2010, pp. 563-567.

[6] O. Fonseca et al., "Identifying Networks Vulnerable to IP Spoofing," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, 2021, pp. 3170-3183, doi: 10.1109/TNSM.2021.306 1486