IP 스푸핑 기반 DoS 공격의 대응 방안 및 고찰

차정훈, 권병욱, 박종혁
서울과학기술대학교 컴퓨터공학과
e-mail:{ckwjdgns, rnjsqud123, jhpark1}@seoultech.ac.kr

IP spoofing based DoS Attack Countermeasures and Consideration

Jeong Hun Cha, Byoung Wook Kwon, Jong Hyuk Park
Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

서비스 거부 공격 (Denial of Service: DoS)은 매년 사이버 테러 이슈로 떠오르고 있는 대표적인 공격 양상 중의 하나이다. DoS 공격은 오래된 공격 유형으로 이에 대응하기 위한 연구가 많이 진행되고 있지만, IP(Internet Protocol) 주소를 변조할 수 있는 프로토콜 취약점 때문에 공격 발신지 역추적에 어려움이 있으며 DoS 공격의 다양한 성장으로 이어지고 있다. 현재 대부분의 변형된 DoS 공격들은 IP 주소를 변조하는 IP 스푸핑에 기반하고 있다. 이 때문에 익명성을 이용하여 공격 시도가 지속적으로 발생하고 있으며 정상적인 사용자와 공격자 간의 구분이 불분명하여 방어하기가 어렵다. 그렇기 때문에 본 논문에서는 여러 변형된 DoS 공격 유형 및 IP 스푸핑을 방지하기 위한 연구들을 분석함으로써 향후 공격자의 역추적을 돕고 DoS 공격을 차단하기 위해 필요한 정보를 제공한다.

1. 서론

정보화 기술 발전에 따라 인터넷은 보편적으로 사용하고 있는 기술이 되었으며 개인, 기관뿐만 아니라 정부 공공기관에서도 쓰인다. 이러한 중요성 때문에 사이버 침해사고로 인한 피해가 불편함을 넘어서 막대한 국가적인 손실로 이어지고 있다. 이때, 시스템을 마비시키는 목적으로 가장 많이 사용되는 공격 유형이 서비스 거부 (Denial of Service: DoS) 공격이다.

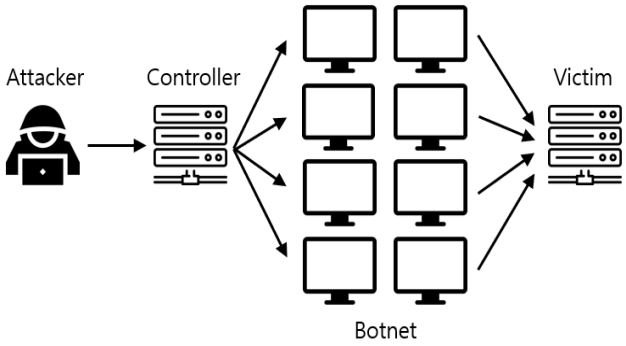
DoS 공격은 악의적으로 상대 시스템 자원을 고갈시켜 원래 의도한 용도로 사용하지 못하게 만드는 정보보안의 필수 요소 중 가용성을 침해하는 공격으로 사용자가 적절한 시간에 인가된 당사자에게 정상적인 서비스를 이용하지 못하게 하는 것을 목적으로 한다. 이때 비정상적인 네트워크 성능 저하, 특정 웹사이트의 접근 불가, 특정 전자우편의 급속한 증가를 야기할 수 있다[1]. DoS 공격은 공격 방법에 따라 분산 서비스 거부 (Distributed Daniel Of Service: DDoS) 및 분산 반사 서비스 거부 (Distributed Reflection Danel Of Service: DRDoS) 공격 등으로 발전한다. DDoS 공격은 공격자가 자신의 컴퓨터로 직접 공격하는 DoS 공격과 다르게 봇넷(Botnet)을 운용하여 공격자의 정보 역추적을 어렵게 하며, 많은 좀비PC의 규모만큼 강력한 트래픽을 발생시켜 공격을 극대화 시킬 수 있다. DRDoS는 발신지 IP 주소를 변조하는 IP 스푸핑 기술을 이용하여 공격에 이용할 서버 반사체(Reflector)에 발신자 IP주소를 타겟 IP주소로 패킷을 보내 반사체가 타겟에게 패킷을 전송하는 공격 방식이다.

2016년 10월 21일 DNS 서비스 제공업체 Dyn이 대규모 DDoS 공격을 받아 서비스가 마비되거나 지연되는 사건이 발생했다. 공격 방법은 Mirai 악성코드에 감염된 IoT(Internet of Things) 기기에 의한 DDoS 공격으로 확인됐다[2]. IoT 기기들은 2021년에 210억대를 예측할 정도로 급증하고 있어 보안이 취약한 IoT 기기들이 공격자의 봇넷으로 악용될 문제점으로 대두된다[3].

DDoS 공격은 다양한 프로토콜들의 보안 취약점을 이용한 공격이다. 대표적인 예로 TCP SYN Flooding 공격은 IP 스푸핑을 통해 발신자를 속이고 TCP 3-way Handshake 절차의 취약점을 이용한 공격이다. 해당 공격을 방어하기 위해 발신지 IP를 차단하는 방법을 사용한다. 하지만 실제 IP를 가진 사용자가 정상적인 서비스를 이용할 수 없으므로 완전한 방어 방법이라고 할 수 없다. 이 외에도 DNS(Domain Name System) Flooding, NTP(Network Time Protocol) amplification, SNMP(Simple Network Management Protocol) reflection , UDP(User Datagram Protocol) Flooding 공격 등이 있지만 이런 다양한 공격들은 IP 스푸핑을 사용하는 공통점을 가지고 있다. 따라서 IP 스푸핑 방지 연구는 다양한 DoS 공격을 방어하기 위해 중요하다. 그러므로 본 논문에서는 변형된 DoS 공격과 최근 많이 사용되는 TCP, DNS 취약점을 이용한 공격을 분석하고자 한다. 또한, DoS 공격의 대응 방법으로 진행 중인 여러 IP 스푸핑 방지 기술들을 분석하고 향후 연구 과제에 대하여 기술한다.

2. 관련 연구

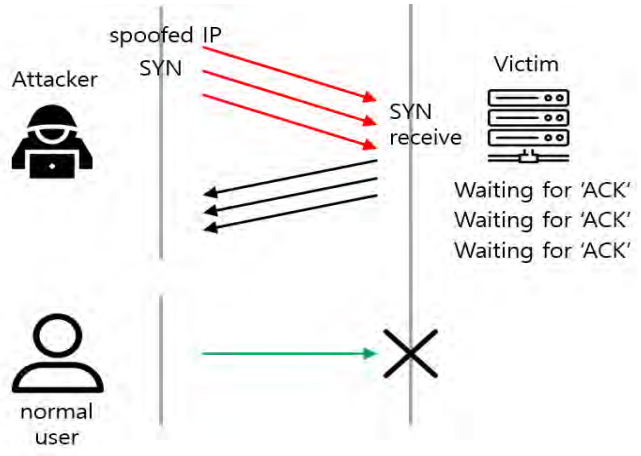
DoS 공격은 서버의 리소스를 고갈시켜 클라이언트가 정상적인 서비스를 이용하지 못하게 하는 공격이다. DoS는 공격자가 다양한 프토토콜 취약점을 이용해 직접적으로 공격하기 때문에 네트워크 대역폭을 마비시키기에는 무리가 있다. 하지만 DoS의 단점을 극복하기 위해 DDoS, DRDoS 와 같은 파생 공격 유형들이 보고됐다. DDoS 공격은 DoS 공격의 단점을 보완한 공격으로써 공격자는 자신의 공격을 수행할 봇넷에 C&C(Command&Control) 서버를 통하여 공격 명령을 내리며, 봇넷의 규모가 커짐에 따라 대량의 트래픽을 발생시킬 수 있다. 공격 형태는 (그림 1)과 같다. DRDoS는 DDoS보다 더 발전된 형태이다. DRDoS는 정상적으로 서비스를 제공하는 서버들에게 발신지 IP를 공격 대상 IP로 위장해 응답이 대상 IP로 반사되어 공격하는 특징을 가진다. DRDoS는 응답 패킷을 증폭시켜서 적은 자원으로 대량의 트래픽을 발생시킨다.



(그림 1) DDoS 공격 형태

2.1. TCP Flooding 공격 분석

전송 계층 취약점으로 대표적인 TCP의 통신 절차 3-way Handshaking의 취약점을 이용한 TCP SYN Flooding 공격이다. TCP SYN Flooding 공격은 세션 연결을 위한 3-way Handshaking 절차 과정에서 마지막 ACK 응답을 하지 않음으로써 상대방 시스템 리소스를 고갈시키는 공격이다[5].

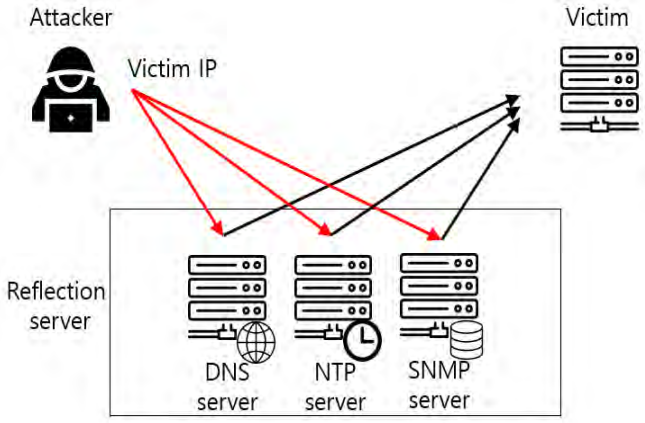


(그림 2) TCP SYN Flooding 동작 과정

(그림 2)는 TCP SYN Flooding 공격 과정을 나타낸다. TCP Flooding은 SYN 플래그뿐만 아니라 FIN, ACK, PUSH, RESET, URG 플래그들을 조합한 공격 형태로도 사용된다. Flooding 공격은 플래그의 이상 현상을 탐지하거나 패킷 도착 이후 일정 시간 동안 응답이 없을 경우 해당 세션 연결을 RESET으로 끊고 해당 IP 주소를 차단함으로써 방어할 수 있다. 프록시 방화벽을 이용하여 서버와 직접적으로 통신하기보다 방화벽을 거쳐서 통신하는 대응 방안을 사용하면 IP를 차단하지 않고도 Flooding 공격을 방어할 수 있다[6].

2.2. DNS 증폭 공격 분석

DNS 증폭 공격은 DNS 서버의 취약점을 이용한 공격으로 발신지 IP를 공격 대상 IP로 속여서 DNS 서버의 응답을 공격 대상으로 보내는 DRDoS 형태의 공격이다[7]. (그림 3)은 DRDoS 공격 형태를 나타낸다. DNS 증폭 공격의 특징은 UDP를 사용하며 DNS 질의에 대한 응답 트래픽은 질의 트래픽보다 크기 때문에 적은 자원으로 대량의 트래픽을 만들 수 있다. DNS 공격을 증폭하기 위해 각 DNS 요청은 암호화 기능을 사용하거나 단일 요청으로 DNS 영역에 대한 모든 알려진 정보를 반환하는 “ANY” 유형의 쿼리를 사용할 수 있다. 증폭 쿼리는 약 60바이트의 DNS 요청 메시지로 대상 서버에 4000바이트 이상의 응답을 이끌어 낼 수 있다[8].



(그림 3) DRDoS 공격 형태

3. IP 스푸핑 대응 방안

3.1. Egress, Ingress Filtering

Ingress 필터링은 라우터 내부로 들어오는 패킷의 발신지 IP 주소를 자신의 서비스 대역에 해당하는 IP 주소가 아닐 경우 패킷을 폐기한다. 마찬가지로 Egress Filtering은 내부에서 외부로 나가는 패킷의 속성을 확인하여 조직 내부에 존재하는 공격의 위협이 조직 밖으로 전파되지 않도록 한다[9-10]. 하지만 이 기술들은 같은 네트워크 대역으로 IP 주소가 변조된 경우 탐지가 어렵다.

3.2. uRPF (Unicast Reverse Path forwarding)

포워딩 테이블을 이용하여 패킷을 필터링 하는 방법이다[11]. 인터페이스를 통해 들어오는 패킷의 발신지 IP 주소가 라우팅 테이블 정보로 포워딩할 때 나가는 인터페이스인지 확인한다. 패킷이 들어온 인터페이스와 나가는 인터페이스가 동일하지 않으면 변조된 IP주소로 판단하여 패킷을 폐기한다. 그러나 이 기술은 전송 경로가 대칭을 이루지 않는 비대칭 경로를 통하여 전송되는 경우 정상적인 패킷도 폐기하기 때문에 신뢰성이 낮다.

3.3. HCF (Hop Count Filtering)

패킷 전송 시 IP 헤더에 존재하는 TTL(Time To Live) 값을 검사하는 방법이다[12]. TTL 값은 전송 경로에 라우터를 지날 때 마다 1씩 감소하여 전송에 실패한 패킷이 인터넷 네트워크 내에서 지속적으로 순환하는 상황을 방지한다. 전송받은 패킷의 TTL 값과 초기 TTL 값을 추론하여 계산된 홉 카운트와 값이 다르면 패킷을 폐기한다. <표 1>은 이러한 알고리즘을 나타낸다. 하지만 공격자가 자신으로부터 목표 발신지까지 홉 카운트를 계산하여 IP 헤더의 TTL 값을 변조하면 홉 카운트 필터링을 우회할 수 있다.

```
for each packet:
    extract the final TTL T and IP address S;
    infer the initial TTL T_o;
    compute the hop-count H_c = T − T_o;
    index S to get the stored hop-count H_s;
    if (H_c ≠ H_s)
        packet is spoofed;
    else
        packet is legitimate;
```

<표 1> Hop-Count inspection algorithm

3.4. PPM (Probabilistic packet marking)

PPM 기술은 패킷이 지나온 전송 경로를 역추적하기 위해 일정 확률로 패킷의 IP 헤더의 Identification 필드에 지나온 라우터 정보를 마킹하는 기술이다[13]. 지나온 모든 라우터의 정보를 마킹하게 되면 처리하는 라우터와 네트워크의 부하가 심해지므로 일정 확률에 의해서 마킹한다. 그렇기 때문에 공격 경로를 역추적하기 위해서 많은 패킷의 양이 필요하다. 대량의 트래픽을 유발시키는 DoS 공격에 적합할 수 있지만 높은 오탐율을 가지며 공격자의 덮어쓰기로 인해 올바르지 않은 정보를 수신할 수 있다.

3.5. DPM (Deterministic packet marking)

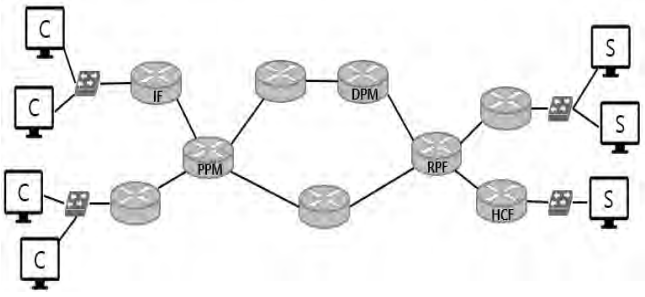
DPM 기술은 지나온 전송 경로의 모든 라우터 정보를 IP 헤더의 Identification 와 Flag 필드에 마킹한다[14]. 하지만 필드의 크기가 17비트이므로 마킹할 공간이 부족하다. 그래서 라우터는 자신의 인터페이스 주소를 임의의 수로 나누어 랜덤으로 기록한다. DPM은 모든 패킹 마킹하기 때문에 PPM과 비교하면 네트워크의 부하가 심하지만, 공격자가 packet marking을 고려해서 Identification 공간을 임의로 조작하더라도 전송 경로상의 라우터가 덮어쓰기 때문에 PPM과 비교했을 때 더 신뢰성이 높다.

4. 현재 연구 이슈 및 고찰

현재 많은 해결 방안들이 제시되고 있음에도 IP 스푸핑을 이용해 많은 DDoS 공격들이 보고되고 있다. IP 스푸핑 방지 기술은 상호 관련이 있는 여러 측면의 영향을 받는 복잡한 프로세스이기 때문에 운영 및 기술적 요구 사항이 추가로 필요하다. 다음 요구사항들은 [15-17]을 기반으로 다음과 같이 고찰한다.

효율성 : IP 스푸핑 방지 기술은 네트워크 대역폭 마비 공격을 방어하기 위한 목적을 가지고 있지만 보안 솔루션을 적용하게 되면 기존의 통신보다 자원 소모량이 늘어나게 된다. 한 가지 예로 네트워크전송 경로에 있는 모든 라우터가 전송중인 패킷이 도착할 때 마다 ICMP 프로토콜로 메시지를 발생시킨다면 전송 경로를 재구성하여 IP 추적 기능을 할 수 있지만 네트워크 부하가 심할 것을 예측할 수 있다. 그렇기 때문에 실제 네트워크상의 방대한 통신 규모를 고려하여 패킷의 크기를 확장시키거나 패킷 분류에 많은 메모리를 사용하지 않도록 구현해야 한다.

ISP 라우터 간의 협조 : Ingress, uRPF, PPM과 같이 IP 변조를 사전에 방지하거나 피해를 입은 시스템에서 패킷의 전송 경로를 역추적하기 위한 기술들은 각 라우터에서 서로 다른 방지 기술들이 사용될 때 효과가 떨어질 수 있다. (그림 4)는 클라이언트(C)와 서버(S) 사이의 9개 노드 네트워크에서 서로 다른 IP 스푸핑 방지 솔루션을 사용하는 네트워크 구성도를 나타낸다. 서로 다른 IP 스푸핑 방지 기술들은 개별적으로 동작할 때 정확도가 떨어지기 때문에 네트워크에서 같은 솔루션을 사용하여 협력 작용으로 솔루션의 정확도 상승효과를 얻어야 한다.



(그림 4) 서로 다른 IP 스푸핑 방지 기술을 동작하는 네트워크 구성도

배포와 적용성 : DoS 공격은 가용성을 침해하고 치명적인 결과를 야기하기 때문에 필수적으로 방어해야 하지만 DoS 공격은 개별 호스트에 대한 드문 공격일 수 있다. 그렇기 때문에 경제적 규모가 크지 않은 기업에서는 DoS

방어 솔루션에 대한 투자가 적을 수 있으며 이를 해결하기 위해 우선적으로 ISP가 IP 방지 메커니즘을 구축해야 한다. ISP 엣지 라우터 간 협력이 충족되지 않을 때 기업에서 DoS 공격을 방어하기 위한 솔루션은 아키텍처가 복잡하거나 비용이 높으면 적용에 어려움이 생길 수 있다.

5. 결론

DoS 공격은 IP 조작을 기본으로 공격자를 숨기며 다양한 공격으로 공격 대상을 공격하게 된다. 사용자의 편의성을 위한 기술들은 공격자에 의해 악용되며 방어를 위한 기술들과 복합되어 다른 공격으로 변형되며 변형된 공격들을 사전에 모두 방어하기엔 한계가 있다. 하지만 DoS 공격에는 IP 스푸핑이 공통적으로 사용되므로 이를 방지함으로써 대부분의 공격을 방어하기 위해 IP 스푸핑 방지 연구가 필요하다. 본 논문에서는 DoS 공격을 방어하기 위한 해결책으로 여러 IP 스푸핑 방지 기술을 분석했다. 궁극적으로 개별 호스트들이 안티 스푸핑 솔루션을 통해 방어하기보다 ISP 간의 협조를 통해 엣지 라우터 간 IP 변조를 막을 수 있는 기술들의 연계 효과를 이끌어 내는 것이 DoS 공격을 예방할 수 있는 방향이라고 생각한다. 향후 연구 과제로 IP 스푸핑 방지를 위한 연구들이 ISP 엣지 라우터에서 IP 스푸핑 방지 기술을 수용하기 위해 네트워크 통신에 효율적이고 구현이 복잡하지 않아 쉽게 적용할 수 있는 목적으로 발전되어야 할 것 이다.

Acknowledgement

- This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00644, Linux Malware Dynamic Detection & Protection Solution on Embedded Device).

참고문헌

[1] NCCIC, “Understanding Denial-of-Service Attacks”, https://www.us-cert.gov/ncas/tips/ST04-015, Access by Mar. 2019.

[2] 한국인터넷진흥원(KISA), “2016년 Mirai 악성코드 동향”, https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=24864, Access by Mar. 2019.

[3] ERICSSON, “ERICSSON MOBILITY REPORT”, https://www.ericsson.com/assets/local/mobility-report/documents/2016/Ericsson-mobility-report-june-2016.pdf, Access by Mar. 2019.

[4] Timur Ibragimov, Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, “DDoS attack in Q2 2018”, https://securelist.com/ddos-report-in-q2-2018/86537, Access by Mar. 2019.

[5] Eddy, Wesley M. "Defenses against TCP SYN flooding attacks." The Internet Protocol Journal 9.4, pp. 2-16, 2006.

[6] Kavisankar, L., et al. "Efficient SYN Spoofing Detection and Mitigation Scheme for DDoS Attack." 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM). IEEE, pp. 269-274, 2017.

[7] 김정태, 김익균, 강구홍, “은닉형 DDoS 공격 및 대응 기술 동향”, https://ettrends.etri.re.kr/ettrends/162/0905002171/31-6_77-87.pdf, Access by Mar. 2019.

[8] Imperva, “DNS Amplification”, https://www.imperva.com/learn/application-security/dns-amplification/?utm_campaign=Incapsula-moved, Access by Mar. 2019.

[9] Ferguson, Paul, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing.", 2000.

[10] Jong Jin Lee and Ki Young Lee, "A Study of Cloud-based DDoS Attack Defence Mechanism", Journal of KIIT. Vol. 13, No. 10, pp. 91-98, Oct 2015.

[11] Bingyang Liu, Jun Bi, and Athanasios V. Vasilakos. "Toward Incentivizing Anti-Spoofing Deployment", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 3, pp. 436- 450, Mar. 2014.

[12] Wang, Haining, Cheng Jin, and Kang G. Shin. "Defense against spoofed IP traffic using hop-count filtering,“ IEEE/ACM Transactions on Networking, pp. 40-53, Sep. 2007.

[13] Savage, S., Wetherall, D., Karlin, a., and Anderson, T., “Practical network support for IP traceback,” ACM SIGCOMM Computer Communication Review, Vol. 30, No. 4, pp. 295-306, 2000.

[14] Belenky, A. and Ansari, N., “IP traceback with deterministic packet marking,” IEEE communications letters, Vol. 7, No. 4, pp. 162-164, 2003.

[15] Neha Agrawal and Shashikala Tapaswi, “A Lightweight Approach to Detect the Low/High Rate IP Spoofed Cloud DDoS Attacks” IEEE 7th International Symposium on Cloud and Service Computing, pp. 118-123, 2017.

[16] Du Ping and Akihiro Nakao, "DDoS defense deployment with network egress and ingress filtering." IEEE International Conference on Communications, pp. 1-6, 2010.

[17] An, Hyok, Heejo Lee, and Adrian Perrig. "Coordination of anti-spoofing mechanisms in partial deployments." Journal of Communications and Networks, Vol. 18, No. 6, pp. 948-961, 2016.