한국정보전자통신기술학회논문지(jkiiect)'15-10, Vol.8 No.5
논문 15-08-05-429 http://dx.doi.org/10.17661/jkiiect.2015.8.5.429

DRDoS 증폭 공격 기법과 방어 기술 연구

최현상*, 박현도, 이희조

A Study on Amplification DRDoS Attacks and Defenses

Hyunsang Choi*, Hyundo Park, Heejo Lee

요 약 DDoS 공격은 주요 정부기관 및 기업의 서비스 시스템 및 웹사이트를 마비시키는 사이버 공격의 수단으로 지속적으로 이용되고 있다. 최근에는 증폭기법을 이용한 DDoS 공격이 지속적으로 발생하고 있는데 공격의 특징상 다수의 정상적으로 동작하고 있는 서버들에서 공격 트래픽이 발생하므로 정상 트래픽과의 구분이 어렵고 수백 Gbps 이상의 대규모의 공격 트래픽을 발생시킬 수 있으므로 탐지를 하더라도 방어를 하는 것이 매우 어려운 상황이다. 그리고 공격에 이용되는 프로토콜들 중에서 SSDP, SNMP등 일부 프로토콜들은 IoT 장비들에서 널리 사용되는 프로토콜이기 때문에 앞으로 공격에 이용될 수 있는 서버들도 크게 증가할 것으로 예측된다. 본 논문에서는 최근에 인터넷에 커다란 위협이 되고 있는 증폭 기법을 이용한 DDoS 공격들에 대해 이용되는 프로토콜별로 공격 기법을 분석한다. 또한, 공격에 효과적으로 대응하기 위해 공격을 방어하는 네트워크에 공격자가 존재하는 경우, 공격에 사용되는 서버가 존재하는 경우, 공격 대상이 존재하는 경우들로 나누어 각각의 상황에 취할 수 있는 대응 방법을 제안한다.

Abstract DDoS attacks have been used for paralyzing popular Internet services. Especially, amplification attacks have grown dramatically in recent years. Defending against amplification attacks is challenging since the attacks usually generate extremely hugh amount of traffic and attack traffic is coming from legitimate servers, which is hard to differentiate from normal traffic. Moreover, some of protocols used by amplification attacks are widely adopted in IoT devices so that the number of servers susceptible to amplification attacks will continue to increase. This paper studies on the analysis of amplification attack mechanisms in detail and proposes defense methodologies for scenarios where attackers, abused servers or victims are in a monitoring network.

Key Words : Amplification attack, DDoS, IoT, Defense, Security

1. 서론

DDoS(Distributed Denial of Service)란 분산 서비스 거부 공격으로 여러 대의 공격 PC를 이용하여 동시에 특정 서버나 네트워크를 공격하게 하여 해당 서버나 네트워크를 마비시키는 해킹 방법이다. 유명한 예로 2003년도 초에 Slammer 웜에 의해 발생한 대규모 트래픽이 KT DNS서버를 다운시켜 한국에 인터넷이 마비되었던 1.25대란도 DDoS 공격의 일환으로 볼 수 있다. 이후에도 다양한 방식으로 DDoS 공격들이 발생하여 기업과 정부 개인들에게 심각한 피해를 입히고 있다. 다양한 DDoS 공격 방법중에서 분산 반사 서비스 거부 공격(DRDoS: Distributed Reflection Denial of Service) 이라는 기술이 있는데 IP를 기반으로 공격을 방어하거나 공격자 역추적을 어렵게 하기 위해 출발지 IP를 위조(Source IP spoofing)하는 방법을 기존 DDoS 공격에 가미한 방식이다. 즉, 공격자가 공격 타겟의 IP로 자신의 출발지 IP를 변경하여

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0190-15-2011,Development of Vulnerability Discovery Technologies for IoT Software Security)
*Corresponding Author : Department of Computer Science and Engineering, Korea University(realchs@korea.ac.kr)
Received October 8, 2015 Revised October 10, 2015 Accepted October 15, 2015

이를 공격에 이용할 서버 등의 반사체(Reflector)에 보내서 패킷을 전달 받은 반사체가 패킷에 대한 응답패킷을 위조된 출발지 아이피(공격 타겟)로 보내어 DDoS 공격을 수행하는 것이다. DRDoS는 1999년 AusCERT가 공격의 위험성에 대해 경고했었고 실제로 2002년에 처음 공격 사례가 보고되었다.

최근에는 특정 프로토콜의 취약점을 이용하여 트래픽을 증폭시키는 증폭(Amplification) 공격의 형태로 DRDoS 공격이 수행되어 인터넷에 많은 피해를 주고 있다. 특정 프로토콜에서 적은 양의 요청 트래픽에 대해서 큰 사이즈의 응답 트래픽을 전송하도록 설계된 경우가 있는데 이를 취약점으로 DDoS 공격에 이용해 공격의 효율을 극대화 한 것이다. 2014년 2월에 400Gbps 규모의 DDoS 공격이 프랑스에서 발생하였는데 이 공격이 대표적인 증폭 공격 사례 중 하나이다[1].

증폭 DRDoS 공격에는 주로 UDP 프로토콜이 이용되는데 이는 TCP의 경우 3-way handshake 때문에 출발지 아이피가 위조된 상태에서 취약점을 이용한 증폭 공격이 어렵기 때문이다. 실제로 NTP, DNS등 UDP 기반의 프로토콜이 증폭 공격에 널리 이용되고 있다. 그러나 TCP의 3-way handshake 이용해서 증폭 공격을 수행할 수 있는데[14] 이는 프로토콜의 취약점이라기보다는 실제 서비스 구현상의 문제점으로 인해 트래픽의 증폭이 되는 것을 이용한 것이다.

증폭 DRDoS 공격은 좀비 PC들로 구성된 봇넷을 이용하여 수행되는 경우가 일반적이며 공격을 당하는 네트워크의 입장에서는 공격 트래픽이 정상적인 서버(NTP서버, DNS서버 등)에서 오는 트래픽으로 보이므로 이를 단순히 출발지 IP를 기준으로 막아버리면 정상적인 서비스도 마비가 될 수 있다. 게다가 공격이 발생하면 트래픽의 양이 수백 Gbps의 규모까지 될 수 있기 때문에 이를 방어하는 것은 매우 어렵다. 현재 한국에는 5개의 인터넷 교환 센터(IX: Internet Exchange)가 존재하고 한국에서 외국으로 오가는 트래픽이 인터넷 교환 센터를 거치게 된다. 그러나 이들의 용량은 수십 Gbps에서 수백 Gbps로 증폭 공격을 이용해 쉽게 공격이 가능하다. 인터넷 교환 센터가 증폭 공격을 받으면 한국의 인터넷 망 전체가 전 세계 인터넷 망과 단절이 될 수 있으며 이러한 공격이 미래에 사이버전에 이용이 된다면 매우 치명적일 수 있다. 일부 IX 연동구간에 설치된 DDoS 대응 장비로도 보호할 수 없는 상황이다.

기존의 증폭 DRDoS 공격은 주로 NTP나 DNS 프로토콜이 사용되었는데 최근에는 SSDP나 SNMP 프로토콜이 증폭공격에 이용되는 경우가 탐지되고 있다. 이들 프로토콜은 IoT 기기들에 많이 사용이 되고 있어 IoT 기기들의 급격한 증가와 함께 증폭 공격에 이용될 취약한 기기의 수도 급격하게 증가할 것으로 예측된다. 특히 저가의 IoT 장비들은 자동으로 보안 취약점을 패치하기 어려운 경우가 대다수 이므로(사용자가 펌웨어 업데이트를 직접 수행해야 하거나 펌웨어 업데이트 자체가 없는 경우가 많음) 취약점이 노출된 채로 지속적으로 증폭 공격에 이용될 것이므로 이에 대한 대책이 필요하다.

증폭 공격에 이용할 취약한 서버는 공격자가 네트워크 스캐너를 이용하여 검색하는 것이 일반적인데 인터넷에 연결된 디바이스 검색엔진 Shodan[2] 등을 이용하면 더욱 간단하게 증폭 공격에 이용할 취약한 서버의 리스트를 확보할 수 있다.

최근에는 저렴한 가격으로 DDoS 공격 서비스를 제공하는 Booter[3]나 Stresser[3]가 일반 유저들에게 공개되어 있는데 이들 공격은 대부분 증폭 DRDoS 공격을 이용하고 있고 공격에 필요한 비용이 저렴하고(5달러 이하) 웹 인터페이스를 통해 이용하고 결제가 손쉬워(paypal 등으로 결제가능) 일반 사용자들에게 많이 이용되고 있어 인터넷 보안에 큰 문제로 대두되고 있다.

본 논문에서는 먼저 증폭 공격에 대해서 유형

별로 분석한다. 각 프로토콜에서 증폭 공격이 가능한 이유와 공격 기법에 대해 알아본다. 그리고 이러한 증폭공격을 원천적으로 차단할 수 있는 기법들이 있는지 살펴본다. 마지막으로 증폭 공격에 대한 공격 대상이 네트워크에 존재하는 경우, 공격에 사용되는 서버가 네트워크에 존재하는 경우, 공격자가 네트워크에 존재하는 경우들로 나누어 각각의 상황에서 효과적인 증폭 공격 방어 기법을 제안한다.

2. 관련연구

2.1 DDoS 공격 기법

지금까지 다양한 방식의 DDoS 공격 기법들이 연구되고 사용되고 있다[4].

최근에 연구되어 발표된 DDoS 기술들을 살펴보면 우선 DirtJumper[5]라는 공격 기법이 있는데 네트워크 대역폭을 소모하는 기법이 아니라 인터넷 커넥션을 소모하는 공격 기술 이었다. Crossfire[6] 공격 기술의 경우는 봇들로부터 적은 양의 트래픽을 특정 링크에 집중시켜 타겟을 인터넷에서 접속 차단을 시키는 기술이다. Coremelt[7] 공격의 경우 라우팅경로의 정보를 이용해 봇들이 발생시키는 트래픽을 특정 코어 네트워크에 집중시켜 링크를 다운시키는 기술이다.

2.2 DDoS 방어 기법

Pushback[8]이라는 기술은 원치 않는 패킷들을 업스트림 라우터들에서 협력을 통해 차단할 수 있는 기술이다. LADS[9]는 Netflow와 SNMP 기반의 DDoS 트래픽 탐지 시스템이다. 컴퓨터가 풀기 힘든 퍼즐을 이용해서 퍼즐을 푼 정상 사용자에게만 토큰을 부여하는 방식으로 DDoS 공격을 방어하는 기술도 고안되었다[10]. Threshold Random Walk[11]는 sequential hypothesis testing을 이용한 호스트 스캔 및 포트스캔 탐지 기술이다. 이외에도 현재까지 많은 DDoS 공격 방어기술이 개발되어 이용되고 있다[4].

2.2 Amplification 공격 분석

C. Rossow[12]는 현재 까지 발생한 증폭 공격 유형에 대한 분석과 추후 새롭게 이용될 수 있는 프로토콜에 대해서도 분석하였다. Marc et. al.[13]는 증폭 공격의 피해를 최소화하는 기법에 대해서 발표하였다.

3. DRDoS 증폭 공격 기법

DRDoS 증폭 공격은 기존 DRDoS 공격에 트래픽 증폭 원리를 가미한 공격이다. 공격자는 공격을 수행하기 전에 증폭 공격이 가능한 취약한 서버의 리스트를 확보하거나 직접 찾는다. 확보된 서버들에 출발지 주소를 공격을 수행할 타겟의 주소로 변조하여 패킷을 전송하면 서버들은 증폭된 응답 패킷들을 타겟에 전송하여 서비스 거부 공격이 수행된다.

증폭 공격은 TCP 프로토콜을 이용해서도 수행할 수 있는데[14] UDP를 사용하는 경우가 일반적다. 따라서, 본 논문에서는 UDP를 사용하는 증폭 공격을 중심으로 다루도록 한다.

UDP 기반의 증폭 공격에는 Chargen, NTP, DNS, SSDP, SNMP, NetBios, QOTD, P2P 등의 프로토콜 등을 이용할 수 있다. 각각의 증폭 공격에 어떠한 방법으로 각 프로토콜이 이용될 수 있는지 살펴보도록 하겠다.

3.1 NTP Amplification

NTP(Network Time Protocol)는 가장 오래된 인터넷 프로토콜 가운데 하나로 네트워크를 통해 컴퓨터 간 시간 동기화를 위한 네트워크 프로토콜 이다. Shadowserver[15]의 통계에 따르면 2014년도에 전 세계에 존재하는 NTP 서버(서비스가 열려있는)의 수는 수백만 대 규모였으며 특히 한국에 NTP 서버가 32만대 이상 존재하는 것으로 조사되었다. NTP 프로토콜에서 시간 동기화를 원하는 클라이언트가 NTP 서버에 현재 시간을 요구하는 요청을 클라이언트의 현재 시간을 포함하여 전송하면 서버는 이 요청을

받은 시간과 현재 시간을 패킷에 포함하여 클라이언트에 전송한다. 클라이언트는 기록된 시간 값들을 이용하여 시스템 시간으로 설정한다.

NTP 서버는 “monlist” 라는 명령으로 요청을 받을 수 있는데 이 요청을 받으면 최근에 접속한 최대 600개의 호스트들에 대한 정보를 응답으로 보내준다. 보통 “monlist” 요청은 8 byte로 가능한데 반해 응답은 일반적으로 수백에서 수천 배의 크기가 된다. 이러한 취약점(CVE-2013-5211)을 갖는 서버는 인터넷 상에 다수 존재하고 증폭이 되는 정도가 매우 크기 때문에 증폭 공격에 많이 사용되고 있다. 2014년 2월에 프랑스에서 탐지 되었던 400Gbps 규모의 DDoS 공격도 NTP 프로토콜을 이용한 증폭공격 사례이다. NTP는 UDP 123번 포트를 이용하고 NTP 서버들은 nmap 등의 스캐닝 툴을 이용하여 쉽게 찾을 수 있다.

3.2 DNS Amplification

DNS(Domain Name System)는 호스트의 도메인 이름을 아이피 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 만들어진 주소 변환 프로토콜이다. DNS 서버들은 거대한 계층적 구조를 갖고 있으며 DNS 레코드 값을 서버에 재귀적인 방식으로 질의를 하여 찾을 수 있다. Shadowserver의 통계에 따르면 전 세계에 수백~수천만대의 DNS 서버가 존재하며 특히 한국에 존재하는 DNS 서버의 수는 45만대가 넘는 것으로 알려져 있다. DNS서버에 질의를 할 때는 어떠한 종류의 레코드 값을 알고자 하는지 알려주기 위해 레코드 타입을 명시한다. A타입(IP Address), MX(Mail Exchange) 등 수십여 개가 넘는 레코드 타입이 존재하는데 이중에서 질의를 보낼 때 ANY 타입으로 보내면 DNS서버는 질의를 받은 도메인과 관련된 모든 타입의 레코드 정보를 보내준다. 증폭 효과가 커서 공격에 자주 이용되는 질의 도메인으로는 ripe.net 등이 이다. 이러한 취약점(CVE-2006-0987)은 비교적 오래전(2006년)에 발견되었는데 최근까지도 증폭 공격에 널리 이용되고 있다. 특히 기존의 DNS 프로토콜은 512byte로 사이즈 제한이 있었으나 기존 프로토콜의 확장 버전인 EDNS의 경우는 4096byte까지 전송이 가능하여 더 큰 증폭 효과를 만들 수 있다. DNS는 UDP 53번 포트를 이용하고 DNS 서버에 dig 명령을 이용해 ANY 타입의 쿼리를 보내 취약한 서버를 찾을 수 있다.

3.3 SSDP Amplification

SSDP(Simple Service Discovery Protocol)는 UPnP(Universal Plug and Play) 프로토콜에서 근거리 혹은 인터넷에 연결된 디바이스를 찾는데 사용되는 프로토콜이다. SSDP를 이용해 DHCP나 DNS와 같은 네트워크 서버나 정적인 호스트 설정 없이 디바이스 탐지가 가능하다. 라우터, 미디어서버, 웹캠, 스마트 티비, 프린터 등의 장비들에서 널리 사용되고 있으며 앞으로 IoT 장비들에도 널리 사용될 것으로 예상된다. Shadowserver의 통계에 따르면 전 세계에 수백~수천만대 규모의 SSDP 서버가 동작하고 있으며 한국에도 25만대 이상의 SSDP 서버가 존재한다. SSDP 프로토콜에서 M-Search 메서드를 이용하면 멀티캐스트 방식으로 로컬네트워크에 연결되어 있는 디바이스를 찾을 수 있는데 이때 응답 패킷에는 헤더와 배너정보 OS, UUID 정보 등, 다양한 정보들이 포함되는데 40byte 정도의 M-Search 요청에 대해 서버는 평균적으로 30배 이상의 크기를 갖는 응답을 보내준다. UDP 1900번 포트로 SSDP M-Search 패킷으로 인터넷을 스캐닝 하여 SSSDP 서버들을 찾을 수 있다.

3.4 SNMP Amplification

SNMP(Simple Network Management Protocol)는 라우터, 스위치, 서버, 워크스테이션, 프린터 등 네트워크 디바이스를 관리하는 목적으로 만들어진 프로토콜이다. 네트워크 디바이스의 모

니터링은 ICMP와 같은 프로토콜을 사용했었으나 네트워크가 복잡해지면서 ICMP만으로 네트워크 디바이스 관리를 효율적으로 할 수 없게 되어 새롭게 만들어진 프로토콜이다. SNMP 프로토콜을 이용하면 네트워크 구성관리, 성능관리, 장비관리, 보안관리가 가능하다. Shadowserver의 통계에 따르면 전 세계에 수백만 대 규모의 SNMP 서버가 존재하며 한국에서도 23만대 이상의 SNMP 서버가 존재한다. 장비 관리에 접근제어는 SNMP 패킷의 community 필드의 값으로 하게 되는데 보통 public과 같은 값으로 세팅되어 있다.

SNMP 프로토콜에서 GetBulkRequest 명령을 이용하면 테이블에 있는 객체데이터를 요청하는 GetNextRequest 명령을 반복적으로 수행하게 된다. 대략 70 byte의 GetBulkRequest 요청으로 최대 수만 byte의 응답을 받을 수 있다. SNMP는 UDP 161번 포트를 이용하며 community 값을 public으로 SNMP 패킷을 생성해 스캐닝을 하면 증폭 공격에 이용 가능한 SNMP 서버들을 찾을 수 있다.

3.5 CharGen Amplification

CharGen(Character Generator Protocol)은 클라이언트의 요청에 대해 랜덤한 개수(0-512)의 문자열을 응답으로 보내주는 프로토콜이다. 네트워크 연결에 대한 디버깅, 대역폭 테스팅 등에 사용되었다. Shadowserver의 통계에 따르면 최근에도 수만 대 규모의 CharGen 서버가 인터넷에 존재하는 것으로 알려져 있는데 한국에는 1500대 정도의 서버가 존재한다. 60byte의 요청 패킷에 대해서 랜덤한(74 ~ 1472 bytes) 크기의 응답을 보내주므로 평균적으로 수백 배 정도의 증폭효과를 갖는다. UDP 19번 포트를 이용하며 nmap등의 스캐닝 툴을 이용해 CharGen 서버를 찾을 수 있다.

3.6 Other Amplifications

앞서 설명한 프로토콜들 외에도 증폭 공격에 이용할 수 있는 프로토콜들은 다수 존재하는데 윈도계열 운영체제에서 PC의 이름 등록(name registration) 과 resolution을 수행하는 NetBIOS 프로토콜의 디버깅을 위한 nbtstat 명령을 이용하면 약 3배 정도의 증폭 효과를 갖는 증폭 공격을 할 수 있다.

QOTD(Quote Of The Day)는 UDP 17번을 사용하는 프로토콜로 오늘의 명언을 요청하는 호스트에게 전달할 수 있는데 CharGen 프로토콜과 거의 유사한 형태로 증폭 공격에 이용 가능하다.

그 밖에도 BitTorrent의 해쉬 탐색, KAD의 피어(peer) 리스트 교환 메시지, 네트워크 게임의 P2P 프로토콜에서 게임서버에 현재 상태 질의 등을 이용해서 증폭 공격을 수행할 수 있다.

표 1. Amplification 프로토콜 비교
Table 1. Comparison of Amplification Protocols

Protocol	UDP Port	Amplification Request	Amp. Factor	Abusable Servers
NTP	123	get monlist	≒206	Millions
DNS	53	ANY query	≒50	>20Millions
SSDP	1900	M-search	≒30	Millions
SNMP	161	GetBulkRequest	≒650	Millions
CharGen	19	(Random)	≒360	90K

이와 같이 다양한 UDP 프로토콜들을 이용하여 증폭 공격을 수행할 수 있는데 각 프로토콜별로 사용하는 포트 값, 증폭 정도, 이용 가능한 서버의 수는 [표 1]에서 확인할 수 있다.

4. DRDoS 증폭 공격의 방어 기법

4.1 Proactive Attack Prevention

사전에 DRDoS 증폭 공격을 방어하는 방법은 1) IP spoofing을 원천적으로 막는 안티스푸핑(Anti spoofing) 기법을 적용하는 방법과 2) 프로토콜 취약점을 패치하는 방법으로 나눌 수 있다.

4.1.1 안티 스푸핑 (Anti-Spoofing)

안티스푸핑 기법을 이용하면 DRDoS 공격을 원천적으로 불가능하게 할 수 있다. 안티스푸핑 기법은 인증 기법을 이용한 방법과 네트워크 토폴로지를 이용한 방법으로 나누어 볼 수 있다.

인증을 이용한 안티스푸핑 기법은 다시 세션 토큰을 이용한 인증, 암호화 기법을 이용한 인증, 제삼자(third-party)를 이용한 인증 등의 방법이 있다. 세션토큰을 이용한 기법은 기법 자체가 증폭공격에 다시 활용될 수 있는 등의 한계점을 갖는다[20]. 암호화를 이용한 인증[21]은 세션토큰을 이용한 인증보다 더 안전한 기법이라 할 수 있으나 암호화 때문에 추가로 드는 성능상의 오버헤드나 추가적으로 트래픽이 발생하는 단점을 갖는다. 제삼자(third-party)를 이용한 인증은 이중에 가장 큰 성능 오버헤드와 추가트래픽이 발생한다.

네트워크 토폴로지를 이용한 안티스푸핑 기법은 IP 헤더를 이용한 방법, 인그레스/이그레스(ingress/egress) 필터링[16], BGP와 라우팅 테이블을 이용한 기법 등이 있다. IP 헤더를 이용한 기법은 대표적으로 IP 헤더의 TTL 값을 체크해서 실제 토폴로지 상에서 가질 수 없는 값을 가질 경우 필터링하는 방법인데 쉽게 우회가 가능하다는 단점을 갖는다. ingress/egress 필터링은 출발지 주소가 정당한 IP 주소 범위에 있는 경우에 트래픽이 네트워크에 들어가거나 나가는 것을 허가하는 방법이다. DPF(Distributed Packet Filtering)[17]와 같은 BGP 라우팅 정보를 이용하여 출발지, 목적지 IP가 불일치하는 경로를 지나는 패킷을 스푸핑으로 판단하는 방법도 존재한다.

4.1.2 Protocol Patch

증폭 공격의 방어를 위해 증폭 공격에 취약한 프로토콜 패치를 하는 방법이 있을 수 있다. 예를 들어 NTP amplification 공격의 경우는 monlist 기능을 제거한 NTP 4.2.7 이후 버전으로 서버를 패치하면 서버가 공격에 이용되는 것을 막을 수 있다. 그러나 이러한 방법은 패치 할 권한이 있는 내부 서버에만 적용할 수 있는 방법으로 인터넷 상에 존재하는 많은 수의 서버가 예전 버전을 그대로 사용하고 있는 현 상황에서 공격을 방어하는 근본적 기술이라고 하기는 어렵다.

4.2 Defense Mechanisms

본 논문에서는 DRDoS 증폭 공격에 대한 방어 기법으로 1) 공격자가 모니터링 네트워크 내에 있을 때 이를 탐지하여 차단하는 방법, 2) 공격에 이용되는 서버가 모니터링 네트워크 내에 있을 때 서버들을 공격에 이용되지 않게 보호하는 방법, 3) 공격 타겟이 모니터링 네트워크 내에 있을 때 공격을 방어하는 기법을 제안한다.

4.2.1 공격자 발생 트래픽 차단

내부 네트워크에서 공격자가 증폭 공격을 하기 위해 발생하는 트래픽을 차단하여 내부 네트워크에서 시도되는 공격을 사전에 차단할 수 있다. 즉 공격자가 직접 혹은 감염된 PC를 이용하여 취약한 서버에 출발지 주소를 스푸핑하여 전송하는 패킷을 차단하는 것이다. IPS(Intrusion Prevention System)와 같은 장비에서는 내부 네트워크의 IP 주소 영역을 알고 있기 때문에 출발지 IP를 스푸핑하여 NTP나 DNS와 같은 취약한 프로토콜을 이용한 패킷이 전송되면 이를 탐지하여 사전에 차단하는 것이 가능하다.

4.2.2 내부 서버 이용 증폭 공격 시도 차단

내부 네트워크에 존재하는 취약한 서버를 이용하여 증폭 공격을 시도하는 트래픽을 탐지하여 차단하면 내부 서버가 증폭 공격에 이용되는 것을 막을 수 있다.

네트워크에 존재하는 취약한 서버를 탐지하는 방법은 알려진 취약한 프로토콜을 이용하는 서버를 스캐닝을 하여 탐지하는 방법과 스마트 퍼

징[18] 기법을 이용한 프로토콜 퍼징을 수행하여 (증폭 공격 관련 취약점은 디버거 대신 incoming/outgoing 트래픽의 비율을 검사하여 찾을 수 있음) 알려지지 않은 취약점을 새롭게 찾아낼 수도 있다.

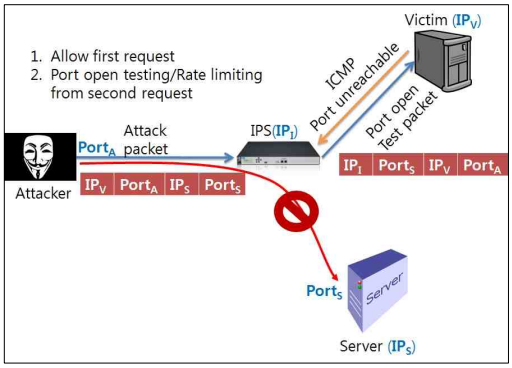

그림 1. 증폭 공격 시도 차단으로 내부서버 보호
Fig. 1. Protecting internal servers from being used as amplification attack amplifiers(reflectors)

이러한 방법으로 찾아낸 취약한 서버들에 외부에서 패킷이 전송되면 첫 요청 패킷에 대해서는 내부 서버로 전달해 줘서 정상적인 통신이 되도록 한다. 이는 모든 패킷에 대해서 테스트나 검사 과정을 거치면 정상적인 통신에 성능이나 기능상에 문제가 생기기 때문이고 일반적으로 정상적인 경우에는 일정 시간 내에서는 하나만의 요청 이 오는 경우가 대부분이고 공격의 경우에는 하나 이상의 요청이 오는 경우가 많기 때문이다. 이후, 일정 시간(수초) 내에 같은 IP로부터 내부 서버에 다시 요청 패킷이 전달되면 [그림 1]에서와 같이 방어 시스템에서 패킷 전송자에 포트가 열려있는지 확인하는 패킷을 전송해서 돌아오는 응답을 보고 포트가 열려있는지 닫혀 있는지 확인한다. 포트가 닫혀 있다면 ICMP port unreachable과 같은 메시지가 전송될 것이고 이의 경우 높은 확률로 전송자의 IP가 스푸핑 되었음을 유추할 수 있다. ICMP 메시지를 받지 못한 경우에는 공격이 아닌 정상 사용자이거나 스푸핑되었으나 타겟의 네트워크에 IPS 장비나 NAT 등에 의해 ICMP 메시지가 차단된 상황을 생각해 볼 수 있다. 이러한 경우는 rate limit 기법을 이용해 일정 시간 내에 임계치 이상의 요청이 들어오면 해당 패킷을 차단하는 방법을 이용할 수 있다. 이러한 방식으로 내부 네트워크의 서버가 증폭 공격에 이용되는 것을 막을 수 있다.

4.2.3 공격 트래픽 차단/감내

내부 네트워크가 증폭 공격을 당하는 경우는 가장 방어가 어려운 경우이다. 왜냐하면 공격의 특성상 수백 Gbps의 대규모 트래픽이 발생되므로 이를 보안 장비가 분석하는 것이 어려울 뿐만 아니라 처리 대역폭이 적은 라우터가 중간에 연결된 경우에는 보안 장비에 트래픽이 도달하기 전에 이미 라우터가 동작불능 상황에 빠지는 경우가 많기 때문이다. 웹 서비스나 서버를 보호하기 위해서는 CloudFlare[19]와 같은 CDN(Content Delivery Network) 기반의 DDoS 방지 솔루션을 제공하는 서비스를 이용하는 것이 가장 좋은 방법이 될 수 있다. 일반 유저의 경우 자신의 실제 IP를 숨기는 방법 등으로 공격을 예방하는 방법을 사용할 수 있다.

5. 결론

최근에는 갈수록 증가하는 증폭기법을 이용한 DDoS 공격에 의해 많은 피해가 발생하고 있다. 증폭 공격의 트래픽은 정상 트래픽과 구분이 어려워 탐지가 어렵고 대규모의 트래픽이 발생하므로 방어 또한 매우 어렵다. 특히, 공격에 이용되는 프로토콜들 중에서 SSDP, SNMP등은 저가의 IoT 장비들에서도 많이 이용되고 있는데 이런 장비들은 자동으로 보안 취약점을 패치하기 어려운 경우가 대부분 이므로 취약점이 노출된 채로 지속적으로 증폭 공격에 이용될 가능성이 높다. 따라서 네트워크상에서 증폭 공격을 탐지 및 방어할 수 있는 방법들에 대한 연구가 필요하다. 본 논문에서는 증폭 공격에 효과적으로

대응하기 위한 방법들을 제안하였다. 공격을 근본적으로 방어할 수 있는 안티스푸핑, 프로토콜 패치의 기법이 있다. 공격을 방어하는 네트워크에 공격자가 존재하는 경우 출발지 IP 스푸핑 패킷의 차단하는 방법으로 방어가 가능하다. 네트워크 내부 서버가 공격에 사용되는 것을 막기 위해서는 내부서버 이용시도를 확인 패킷 전송 및 rate limit 기법을 이용해 탐지 및 차단하는 방법을 제안하였다. 내부 네트워크가 공격을 당하는 경우에는 클라우드 및 CDN 서비스를 이용한 감내 등의 방어 기법을 제안하였다. 이와 같은 방법들을 통해 증폭 공격에 대해 효과적인 방어가 가능할 것으로 기대된다.

REFERENCES

[1] https://blog.cloudflare.com/technical-details-behind - a-400gbps-ntp-amplification-ddos-attack/

[2] Shodan, networked device search engine, http://www.shodanhq.com/

[3] Karami, M., McCoy, D. “Understanding the Emerging Threat of DDoS-as-a-Service”, Proc. of the 6th UNSENIX Workshop on Large-Scale Exploits and Emergent Threats. (LEET), 2013.

[4] J. Mirkovic , P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms”, ACM SIGCOMM, 2004.

[5] M. M. Andrade and N. Vlajic, “Dirt jumper: A key player in today's botnet-for-ddos market”. IEEE WorldCIS, 2012.

[6] M. S. Kang, S. B. Lee, and V. D. Gligor, “The Crossfire Attack”, Proc. of IEEE Security and Privacy (S&P), 2013.

[7] A. Studer and A. Perrig, "The Coremelt Attack", Proc. of the European Symposium on Research in Computer Security (ESORICS), 2009.

[8] J. Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", Proc. of Network and Distributed System Security Symposium (NDSS), 2002

[9] V. Sekar, N. G. Duffield, O. Spatscheck, J. E. van der Merwe, and H. Zhang, "LADS: Large-scale Automated DDoS Detection System", Proc. of the USENIX Annual Technical Conference (ATC), 2006.

[10] X. Wang and M. K. Reiter, "Mitigating BandwidthExhaustion Attacks Using Congestion Puzzles", Proc. of the 11th ACM Conference on Computer and Communications Security (CCS), 2004.

[11] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing", Proc. of IEEE Symposium on Security and Privacy (S&P), 2004

[12] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse", Proc. of the Network and Distributed System Security (NDSS) Symposium, 2014.

[13] M. Kührer , T. Hupperich , C. Rossow , T. Holz, "Exit from hell? reducing the impact of amplification DDoS attacks", Proc. of the 23rd USENIX conference on Security Symposium, 2014.

[14] M. Kuhrer, T. Hupperich, C. Rossow, T. Holz, "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks", USENIX Workshop on Offensive Technologies (WOOT), 2014.

[15] Shadowserver foundation, https://www.shadowserver.org/

[16] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of

Service Attacks which employ IP Source Address Spoofing", IETF RFC 2827, 2000

[17] K. Park and H. Lee, "On the Effectiveness of Route-based Packet Filtering for Distributed DoS Attack Prevention in Power-law Internets", ACM SIGCOMM, 2001.

[18] S. Gorbunov and A. Rosenbloom, "Autofuzz: Automated network protocol fuzzing framework", IJCSNS International Journal of Computer Science and Network Security, 2010.

[19] https://www.cloudflare.com/

[20] W. Feng, E. Kaiser, W. Feng, and A. Luu, "Design and implementation of network puzzles", Proc. of IEEE INFOCOM 2005.

[21] Y. Gilad and A. Herzberg, "LOT: A Defense Against IP Spoofing and Flooding Attacks", ACM Transaction on Information and System Security, 2012.

저자약력

최 현 상(Hyunsang Choi) **[회원]**

- 2004년 8월 : 고려대학교 컴퓨터학과 학사
- 2006년 8월 : 고려대학교 컴퓨터학과 석사
- 2012년 2월 : 고려대학교 컴퓨터학과 박사
- 2012년 3월 ~ 2013년 2월 : 고려학교 정보통신대 연구교수
- 2013년 3월 ~ 2014년 3월 : U.C. Berkeley 박사후연구원

<관심분야> 네트워크 보안, 시스템 보안

박 현 도(Hyundo Park)

- 2004년 8월 : 고려대학교 컴퓨터학과 학사
- 2007년 2월 : 고려대학교 컴퓨터학과 석사
- 2010년 8월 : 고려대학교 컴퓨터학과 박사
- 2010년 9월 ~ 2011년 9월: Bell Lab 박사후연구원
- 2012년 1월 ~ 2012년 10월: 고려대학교 정보대학 연구교수
- 2012년 11월 ~ 2015년 2월: ㈜코닉글로리 개발팀장
- 2015년 5월 ~ 현재: 고려대학교 정보대학 연구교수

<관심분야> 네트워크보안, 시스템 보안

이 희 조(Heejo Lee)

- 1993년 2월 : 포항공대 컴퓨터공학과 학사
- 1995년 2월 : 포항공대 컴퓨터공학과 석사
- 2000년 2월 : 포항공대 컴퓨터공학과 박사
- 2000년 3월 ~ 2001년 2월: Purdue Univ. 박사후연구원
- 2001년 3월 ~ 2003년 10월 : 안철수연구소 CTO
- 2010년 1월 ~ 2010년 12월 : CMU CyLab 방문교수
- 2004년 3월 ~ 현재 : 고려대학교 컴퓨터학과 교수

<관심분야> 네트워크 보안, 시스템 보안