UDP/ICMP 플러딩 공격에 대한 클라이언트 측 방어 기법 연구

김동훈, 이기영

인천대학교 정보통신공학과

A Study of Client Side Defence Method of UDP/ICMP Attack

Dong-hoon Kim and Ki Young Lee

University of Incheon

E-mail : yarishiro@naver.com

요 약

기존의 DDoS 공격에 대한 방어는 공격을 당하는 서버 쪽에서 이루어졌다. 서버에서는 DDoS 공격을 파악하면 대역폭을 늘리거나 트래픽을 우회, 해당 IP를 차단 또는 해당 포트를 방화벽에서 막아서 방어하는 방식을 많이 취했다. 하지만 스마트 폰 사용자가 늘어남에 따라 스마트 폰까지 좀비가 될 수 있는 현재 시점에서 DDoS 공격은 더욱 방대하고 강력해질 수 있다. DDoS 공격의 피해는 공격 당하는 서버에 국한되지 않고, 좀비가 된 호스트들의 하드 디스크가 파괴되거나, 스마트 폰 좀비의 경우에는 과금이 발생하기 때문에 그 피해는 좀비들까지로 확대되고 있는 추세이다. 따라서 서버 쪽에서만 DDoS를 방어할 것이 아니라, 좀비가 될 여지가 있는 호스트 쪽에서도 DDoS 공격을 예방해야 하는 상황에 이르렀다.

이에 본 논문에서는 좀비가 된 PC 또는 스마트 폰이 DDoS 공격을 수행하는 것을 판단하여 해당 프로세스를 종료시키고 그 정보를 다른 호스트들에게도 알려 백신을 빨리 받게 하는 형태의 방어 기법을 연구한다.

ABSTRACT

Traditional DDoS defence methods are performed at server side which was attacked. If servers detect DDoS attack, they use some methods for defending the attack such as increasing the bandwidth, bypassing the traffic, blocking the IP addresses or blocking the ports by the firewall. But as lots of people use smart-phones, it is possible a smart-phone to be a zombie and DDoS attack could be much more a huge and powerful forms than now. Victims are not only a server but also a host which becomes a zombie. While it performs DDoS attack, zombie smart-phone users have to pay the extra charge. After finish the attack, DDoS try to destroy hard drives of zombie hosts. Therefore the situation is changed rather than to defend DDoS server side only, we should protect a client side who needs to prevent DDoS attacks.

In this paper, we study a defence method that we terminates a process which perform the attack, send the information to different hosts when a zombie PC or smart-phone perform DDoS attacks.

키워드

DDoS, Denial of Service, UDP, ICMP, Flooding

Ⅰ. 서 론

그 동안 DDoS (Distributed Denial of Service) 공격은 개인이나 회사를 가리지 않고 사회에 많은 피해를 가져왔다. DDoS 공격은 점차 진화하고 있는데, 그 수법 뿐만 아니라 피해의 범위가 점점 커지고 있다. 2009년에 발생한 7. 7 DDoS 대란 이후로 DDoS 공격의 피해는 해당 서버 뿐만 아니라, 공격이 끝난 시점부터 좀비 호스트의 하드 디스크의 MBR을 망가뜨려 피해의 범위를 확대시키고 있다.

뿐만 아니라 현재 폭발적으로 늘어나고 있는 스마트 디바이스들 또한 DDoS의 좀비로 만들 수 있는 여지가 생기면서 DDoS 공격의 규모가 더 커질 수 있다는 사실은 자명하다. 이런 스마트 디바이스는 통신의 양이 과금과 직결되기 때문에 좀비가 될 경우 막대한 과금과, 네트워크 과부하가 일어날 수 있다[2].

이런 대규모의 공격은 서버 쪽에서만 대처하기가 힘들뿐더러, 좀비 PC와 좀비 디바이스 모두 피해를 받기 때문에 클라이언트 쪽에서도 방어를 해야 하는 상황에 처하게 되었다.

본 저자는 이전에 HTTP get request 공격에 대해서 클라이언트 측에서 방어하는 기법을 소개한 바 있다[1].

이에 본 논문에서는 클라이언트 측에서 DDoS 공격중 UDP/ICMP Flooding 공격을 감지하고 해당 프로세스를 종료시키면서 사용자에게 알려주어 서버와 클라이언트 모두 방어할 수 있는 기법을 제안한다.

Ⅱ. UDP/ICMP 공격 기법

DDoS 공격 기법은 매우 다양한데 본 논문에서는 UDP와 ICMP를 이용한 공격 기법들을 분석하고 방어한다.

1. UDP Flooding 기법은 대량의 UDP 패킷을 이용하여 대상 호스트의 대역폭을 소모시키는 것이 목적이다.

2. UDP Checksum Error 공격은 임의로 UDP의 비정상적인 패킷을 대상 호스트로 전송하여 과부하를 발생시켜 서비스를 발생하는 공격이다.

3. UDP LoopBack 공격은 송신지와 수신지의 포트를 7(Echo), 17(Quote of the day), 19(Chargen) 으로 동일하게 설정하여 패킷을 발송하여 서로간에 무한 통신을 하는 취약점을 이용한 공격법으로 대상 호스트와 네트워크 자체에 과부하를 발생시키는 공격 기법이다.

4. ICMP Flooding은 공격자가 송신지의 IP 주소를 공격하고자 하는 호스트의 주소로 설정하여 broadcast address로 ICMP echo request 패킷을 전송한다. 하위 시스템들은 ICMP echo reply 패킷을 타겟으로 전송하여 대량의 패킷들이 집중되어 네트워크에 부하가 발생하는 방식이다.

Ⅲ. 제안하는 방어 기법

본 논문에서는 클라이언트 측에서 UDP/ICMP DDoS 공격 유형 각각에 대해서 패킷 카운팅을 통해 DDoS 공격을 효과적으로 막을 수 있는 방법을 제안한다.

각 공격에 대한 탐지 알고리즘은 그림1과 같다.

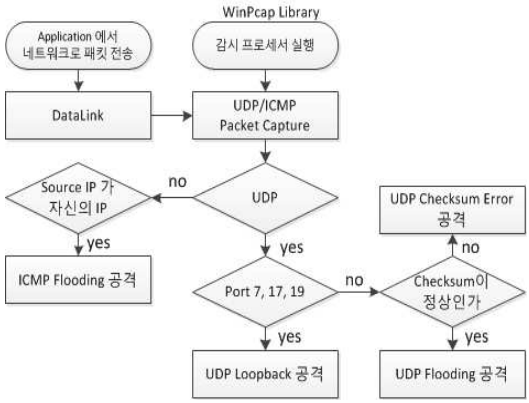

그림1. 공격 탐지 알고리즘

클라이언트에서는 WinPcap 라이브러리를 이용한 DDoS 공격 감시 프로세서를 생성해서 밖으로 나가는 패킷을 캡쳐한다. 밖으로 나가는 패킷 중에서 UDP/ICMP 패킷만을 필터링한다. 패킷의 프로토콜이 UDP인 경우 포트번호를 읽어서 7, 17, 19번인 경우에는 UDP Loopback 공격으로 판단하여 테이블에 삽입한다. 그 외의 포트 번호에 대해서는 체크섬 값을 검사하여 정상이 아닌 경우 UDP Checksum error 공격으로 판단하고, 정상인 경우에는 UDP Flooding 공격으로 판단한다. 프로토콜이 UDP가 아닌 ICMP의 경우 source의 IP를 검사하여 클라이언트의 아이피가 아닌 경우 ICMP Flooding 공격으로 판단한다. 각 공격 경우에 따라 서로 다른 카운팅 임계 값과 시간 임계 값을 적용하여 시간 임계 값 이내에 카운팅 임계 값을 넘는 패킷 카운팅이 발생할 경우에 공격으로 간주하고 해당 프로세스를 종료시키고 사용자에게 어떤 프로세스가 문제를 일으키는지 알려준다. 사용자는 이 정보를 이용해서 해당 프로그램을 삭제하거나, 보안회사에 이 프로그램을 보내 악성코드를 분석하고 보안 패치를 하게 할 수도 있다. 이를 이용하여 서버 쪽에서도 대비를 하게 할 수 있다.

Ⅳ. 결 론

본 논문에서는 클라이언트 측에서 UDP/ICMP Flooding 형태에 대한 공격을 수행할 경우 빠른

시간 안에 이를 탐지하고 해당 프로세스를 종료시킴으로써 클라이언트와 공격당할 서버를 모두 방어할 수 있는 방어기법을 제안하였다.

이런 방어 기법을 일반 사용자들이 사용하는 백신 프로그램에 추가한다면 별도로 사용자들이 이런 프로그램을 설치하지 않고도 효과적으로 DDoS를 방어하는 시스템을 구축할 수 있다.

제안하는 기법은 클라이언트 측에서 동작하는 만큼 서버 측에서도 별도의 비용이 들지 않고, 사전에 방어를 할 수 있다는 장점이 있다.

다만 카운팅 임계 값과 시간 임계 값을 각각의 공격기법에 따라 달리 설정해야 하는 것과 급변하는 네트워크 상태를 고려해야 함은 물론, false alarm detection을 최소화 하기 위해 적절한 임계 값을 찾는 것은 쉽지 않은 일이다.

따라서 향후에는 이 기법을 확장하여 동적으로 임계 값을 설정하여 더욱 효과적으로 공격을 탐지하는 알고리즘을 연구하고 개발해야 할 것이다.

참고문헌

[1] 김동훈, 강수철, 이기영, 클라이언트 측 DDoS 방어 기법에 대한 연구, 한국정보기술학회 2011 추계종합학술대회 논문집, pp.23-27, 2011.

[2] 장기헌, 최상명, 염흥열, "스마트폰 DDoS 공격 동향", 정보보호학회지, 제21권, 제5호, pp.65-70, 2011.