역 IP spoofing을 이용한 DDoS 웜 스캐닝 트래픽 처리기법에 관한 연구

김재용, 김재우, 이영구, 전문석
숭실대학교 컴퓨터공학과
e-mail : {raient, saypeace, ad3927, mjun}@ssu.ac.kr

A Study on DDoS Worm Scanning Traffic Processing Mechanism using Reverse IP Spoofing

Jae-Yong Kim, Jae-Woo Kim, Yung-Goo Lee, Moon-Seog Jun
Dept of Computer Science, Soong-Sil University

요 약

DDoS 공격은 네트워크 보안에 큰 피해를 미치는 공격기법의 하나로써, 국내외로 많은 피해를 유발하고 있으며, 최근에도 DDoS 공격에 의한 피해는 빈번하게 보고되고 있다. DDoS 공격은 실제 공격에 앞서 웜과 악성 BOT을 이용하여 공격을 직접 수행할 호스트를 감염시킨다. 웜과 악성 BOT이 타깃 호스트를 감염시키기 전에 반드시 수행하는 것이 취약점에 대한 스캐닝이다. 본 논문에서는 웜과 악성 BOT의 스캐닝 행위에 초점을 맞추어 DDoS 공격으로부터 안전한 네트워크를 구축하기 위한 역 IP spoofing을 이용한 DDoS 웜 스캐닝 트래픽의 처리기법을 제안한다.

1. 서론

인터넷은 미국 국방부의 고등연구계획국(Advanced Research Project Agency : 약칭 ARPA)의 계획으로 만들어진 세계 최초의 패킷 스위칭 네트워크 ARPnet을 시작으로 끊임없이 발전하여, 현재의 전 세계를 연결하는 광범위한 네트워크를 구축하고 있다. 이러한 인터넷의 발전과 함께 다양한 네트워크 서비스가 제공되고, 이와 더불어 네트워크 보안 공격 또한 끊임없이 발생하며, 공격기법과 피해또한 기하급수적으로 증가 하고 있다.

수많은 네트워크 보안에 대한 위협 중에 웜과 악성 Bot을 이용한 DDoS 공격은 가장 큰 피해를 야기하고 있는 공격기법 중의 하나로서, 수년전부터 최근까지 국외는 물론 국내에서도 그 피해가 계속적으로 보고되고 있다. 2008년에도 국내의 여러 기업의 웹서버가 중국의 DDoS(Distribute Denial of Service) 공격을 받고, 금품을 요구받는 사례가 발생하였다.

DDoS 공격은 공격자가 유포한 웜이 여러 호스트를 감염시켜 희생 호스트에 공격을 수행한다. 웜은 공격자에 의해서 만들어진 프로그램으로서 서비스의 취약점을 이용하여 스스로 네트워크를 통해 스스로 전파하는 특성을 가지고 있다. 특히 네트워크 환경에서의 웜은 빠른 확산속도와 네트워크 자원의 고갈로 큰 피해를 유발하고 있으며, 웜에 대한 탐지 및 방어에 많은 어려움을 겪고 있다.

웜은 확산을 위해서 감염시키기 위한 정상호스트를 탐지하는데 이를 스캐닝이라 하고, 네트워크로 유입되는 전체 TCP SYN 패킷 중에 웜의 스캐닝 패킷으로 의심되는 TCP SYN 패킷의 비율이 평균 90% 이상인 것으로 보고되었다.[1] 실제 공격 트래픽뿐 아니라 웜의 스캐닝 패킷에 대해서 탐지 및 방어를 하여, 최종적인 공격에 대한 보다 효율적인 대응을 할 수 있다.

DDoS 공격이 시작된 후에 웜을 탐지하고, 네트워크 내부의 감염된 호스트를 분류하고 웜의 전파행위를 막고자 하는 연구가 활발히 진행되고 있다.

이에 본 논문은 NAT의 개념을 적용하여, 역 IP spoofing을 이용한 DDoS 웜의 방어 기법을 제안한다. 웜의 탐지에 한하여 기존의 웜 탐지기법을 사용하고, 제안하는 방어 기법을 통해 웜의 전파를 막고 나아가 잠재적인 DDoS 공격의 방어기법을 설명한다.

본 논문의 구성은 다음과 같다. 2 장에서는 DDoS 공격과 웜의 탐지기법에 대한 관련연구를 살펴보며, 3장에서는 역 IP spoofing을 이용한 DDoS 방어기법을 제안하고, 4장에서는 결론 및 향후 연구에 대해 설명한다.

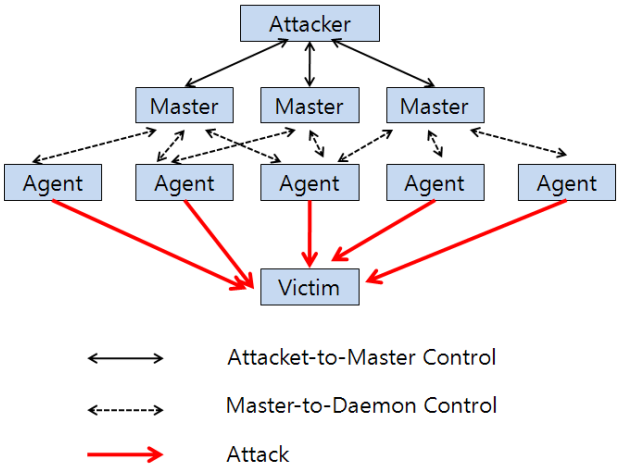
2. 관련연구

본 장에서는 DDoS 공격의 개념을 설명하고, 웜의 특성 및 탐지 기법에 대한 기존 연구를 알아본다.

2.1 DDoS 공격

DDoS 공격은 하나의 공격자가 직접 희생 호스트를 공격하는 것과 달리 공격자가 유포한 웜이나 악성 Bot에

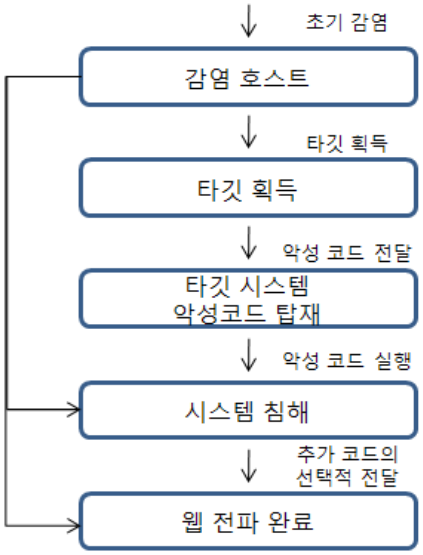
의해 감염된 Master와 Agent 호스트에 의해 여러 방향으로 공격을 감행한다. 그림 1은 DDoS 공격의 일반적인 형태를 보여준다. 공격자는 Master와 Agent 호스트에 원격으로 희생 호스트에 대한 공격을 실행하며 수많은 Agent가 발생한 트래픽은 희생 호스트에게 집중 되어 DDoS 공격을 실행한다.



(그림 1) DDoS공격의 형태

2.2 웜

그림 2는 웜의 일반적인 전파단계로 공격자가 희생 호스트를 공격하기위해 정상 호스트를 감염시키는 프로그램으로서, 스스로 자신을 복제하여 네트워크에 연결된 곳에 확산되는 특징을 가진다. 웜은 정상 호스트를 감염시키기 위해 스캐닝을 실시하며, 스캐닝을 통해 획득한 정보를 토대로 확산을 시작한다. 스캐닝은 TCP SYN 패킷이나 UDP request 메시지를 통해 시행된다.



(그림 2) 웜의 일반적인 전파 단계

먼저 감염 되어진 호스트가 타깃 획득 단계에서 감염시킬 호스트에 대한 스캐닝을 수행한다. 스캐닝을 통해 타깃을 획득 한 후, 해당 시스템이 목적지로 정해지면, 악성코드 전달 단계에서 웜을 전달한다. 실제의 코드 전달은 전자 메일, 네트워크 파일 시스템, 웹 클라이언트 등의 다양한 경로를 통해 타깃으로 유입된다.

2.3 웜의 탐지기법

웜의 탐지기법은 알려진 웜의 정보를 토대로 signature를 생성한 이를 가지고 탐지하는 방식과, 비정상 트래픽 특성 분석을 이용한 탐지 방법으로 분류할 수 있다. 현재 각 연구기관에서 연구되고 있는 웜 탐지 기법을 간략히 살펴보면 다음과 같다.[3], [4], [5]

2.3.1 TRW(Threshold Random Walk)

TRW라는 수학적인 알고리즘으로 트래픽 분석을 통해 웜을 탐지하는 방법이다. 이 방식은 TCP SYN패킷을 스캐닝동작이라고 판다한다는 가정에 TCP SYN패킷의 성공 여부에 따라 스캐닝 여부를 판단한다.

2.3.2 DEWP(Detecting Early Worm Propagation through Packet Matching)

ISI에서 제안한 DEWP방식은 네트워크로 유입되는 트래픽들의 패턴을 특정화 시킨 후에 분류하여 웜을 탐지하는 기법이다. 특정 포트에 일반적인 트래픽량 보다 많은 트래픽이 유입될 때 이를 웜에 의한 스캐닝으로 의심하고 탐지한다.

2.3.3 SID(Statistical Intrusion Detection)

Statistical Intrusion Detection 방식은 통계학적인 방식을 활용하여 웜을 탐지하는 기법이다. 실제 전염병의 확산 방식을 설명할 때 사용하는 Epidemic Model을 사용하여 웜의 탐지에 사용한다. 웜의 모델을 생성하고, 실제 트래픽과 모델의 일치성을 확인하여 탐지한다. CodeRed와 Slammer 웜에 적용하여 탐지하는 기법이다.

2.3.4 AP(Autograph Project)

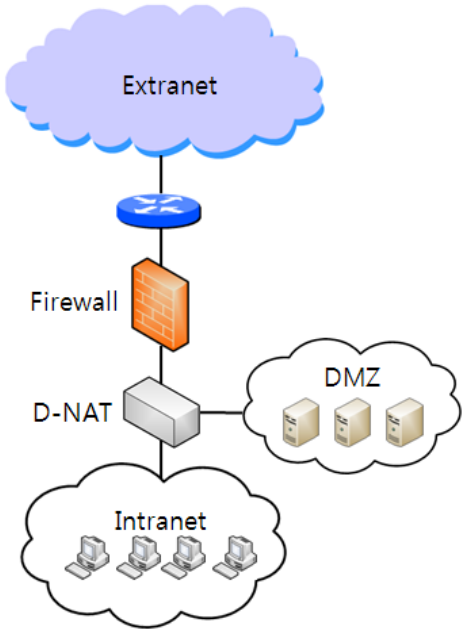
Autograph Project는 Carnegie Mellon University에서 수행하고 있는 웜 탐지 기법으로서, 패킷을 수집하고 자동으로 웜에 대한 signature를 생성하고자 하는데 그 목적이 있다. 비정상 트래픽을 감지하기보다는 웜에 대한 탐지 결과를 참조하여 웜을 탐지한다. 사용되는 알고리즘은 Rabin's Fingerprint로서 모듈러 연산을 이용하여 구현이 쉽고 동작이 빠른 특징을 가지고 있다.

3. 제안기법

본 논문에서 제안하는 기법은 보호하고자 하는 네트워크로 유입되는 트래픽을 분석하여 웜의 스캐닝 패킷을 탐지하고, 스캐닝 트래픽이 보호 네트워크로 유입 되는 것을 차단하는 것에 그 목적이 있다.

3.1 시스템 구성도

제안하는 시스템의 전체 구성도는 그림 3과 같이 네트워크를 보호하는 방화벽 외에 D-NAT(DDoS NAT)를 추가하여, 보호하고자 하는 네트워크로 유입되는 트래픽 을 모니터링 한다. 정상 트래픽과 웜에 의한 스캐닝 트래픽을 탐지하기 위해 기존의 웜에 대한 탐지기법을 사용하고, Firewall과 D-NAT를 통해 Intranet의 inbound 트래픽과 outbound 트래픽을 지속적으로 모니터링 한다.



(그림 3) 제안하는 시스템 구성도

외부에서 내부로 들어오는 모든 inbound 트래픽은 1차 Firewall을 통해 모니터링 되며, 정상 트래픽과 웜에 의한 스캐닝 트래픽으로 분류된다. 정상 트래픽은 방화벽의 기능도 함께하는 D-NAT를 통괄하여 내부의 Intranet으로 유입된다. 웜에 의한 스캐닝 트래픽으로 탐지되는 패킷은 D-NAT를 통해 Intranet으로 유입되는 것을 차단한다. D-NAT는 역 IP spoofing을을 이용한 패킷의 처리뿐만 아니라 일반적인 방화벽의 기능도 함께 수행하면서, inbound 트래픽은 물론, 내부에서 외부로 나가는 outbound 트래픽에 대한 모니터링도 수행한다. 또한 D-NAT에는 기존의 방화벽에서 사용되는 DMZ도 함께 구성이 가능하다. DMZ 또한 1차 Firewall과 D-NAT에 의해 웜에 의한 스캐닝 패킷으로부터 안전하게 보호된다.

3.2 웜 스캐닝 트래픽 처리기법

D-NAT는 Firewall에 의해 탐지된 스캐닝 트래픽을 IP spoofing을 이용하여 처리한다.

Intranet으로 유입되는 목적지의 주소와 포트번호, 패킷의 트래픽량등의 정보를 통해 웜의 스캐닝 패킷으로 의심되는 패킷은 1차 Firewall에서 필터링 되며, 2차 D-NAT를 통해 웜의 스캐닝 패킷에 대한 우회 및 방어를 시행하고, outbound, inbound 트래픽에 대한 모니터링을 수행 하여 웜의 스캐닝 패킷을 탐지한다.

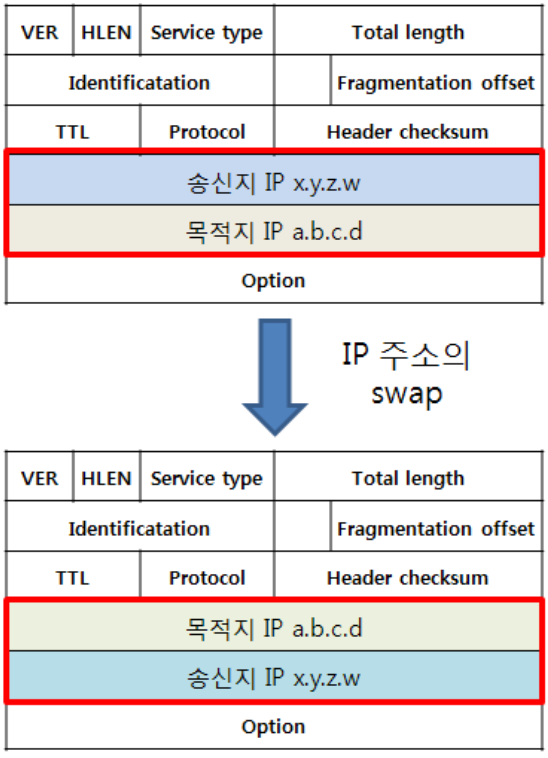
Firewall과 D-NAT의 모니터링으로 정상적인 트래픽은 통과 시키고, 웜의 스캐닝 패킷으로 의심되는 패킷은 D-NAT를 통해 다음과 같은 과정을 거친다.

① D-NAT는 웜의 스캐닝 패킷으로 의심되는 IP 주소를 저장하는 table을 유지한다.

② table에 저장되어 있는 IP 주소를 송신자로 하는 모든 패킷에 대해서 그림 4와 같이 송신지 IP 주소와 목적지 IP 주소를 swap하여 전송한다.

③ Intranet에서 외부로 나가는 outbound 트래픽에 대하여 모니터링 하여 에서 내부 네트워크에서 감염된 호스트에 의한 스캐닝을 탐지한다.

④ outbound 트래픽 중에서도 웜에 대한 스캐닝 패킷이 탐지되면 D-NAT에서 Extranet으로 전송되는 것을 차단한다.



(그림 4) D-NAT의 IP주소 swap

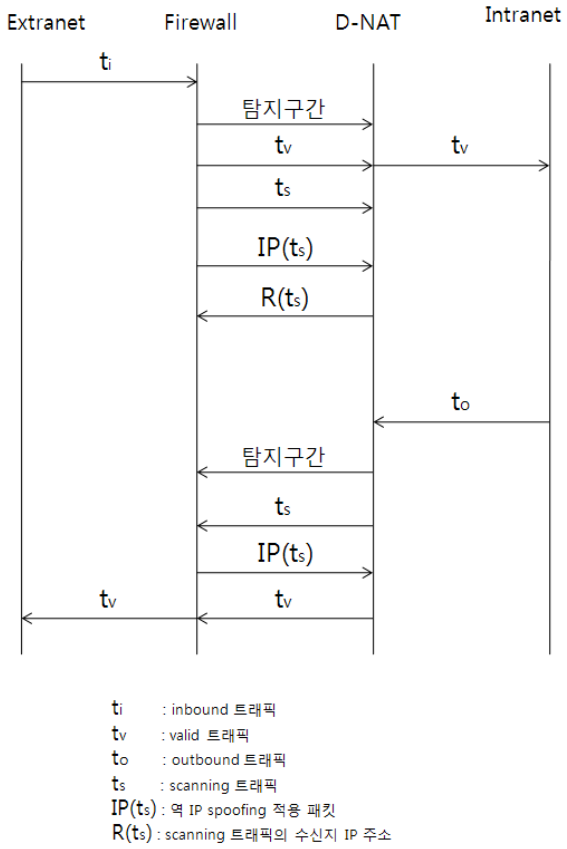
3.3 네트워크 트래픽 흐름도

보호하고자 하는 Intranet으로 유입되는 트래픽에 대한 네트워크 트래픽 흐름도는 그림 5와 같다.

먼저 외부에서 유입되는 inbound 트래픽 t_i는 Firewall과 D-NAT의 탐지구간을 지나가며, 정상적인 트래픽 t_v는 D-NAT를 통해 Intranet으로 유입된다. 반면 스캐닝 트래픽인 t_s는 패킷의 IP 주소를 D-NAT의 table로 전달하고, D-NAT에서 역 IP spoofing을 적용한 패킷 R(ts)를

Extranet으로 전송하는 과정을 거친다.

내부에서 외부로 전송하는 outbound 트래픽 t_o 또한 Firewall 과 D-NAT의 탐지구간을 지나가며, 정상 트래픽과 웜에 의한 스캐닝 패킷을 구별한다. 정상 트래픽 t_v는 D-NAT에서 제약없이 Extranet으로 전송되는 반면, 스캐닝 트래픽인 t_s는 패킷의 IP 주소를 D-NAT의 table로 전달하고, 외부로 나가는 트래픽을 차단당한다.



(그림 5) 네트워크 트래픽 흐름도

웜은 정상 호스트를 감염시키기 위해서 노출된 서비스를 목표로 스캐닝을 시도한다. 본 논문에서 제안하는 기법은 DDoS 공격을 위해서 반드시 선행되는 웜의 스캐닝 행위에 초점을 맞춘 DDoS 공격의 방어 기법이다. 일반적으로 네트워크로 유입되는 약 90%의 스캐닝 패킷에 대한 탐지와 역 IP spoofing을 이용하여 보호대상의 네트워크에 웜의 스캐닝 패킷의 유입을 최소화 한다.

4. 결론

본 논문에서는 현대 네트워크 환경에 큰 위협중의 하나인 DDoS 공격에 대한 방어기법을 제안하였다. DDoS 공격을 위해 선행되는 웜의 스캐닝 기법과 웜의 스캐닝을 탐지하기 위한 기존 연구결과를 기반으로 하여, 역 IP spoofing의 개념을 적용한 D-NAT를 추가하여 네트워크로 유입되는 스캐닝 패킷의 비율을 감소시키고, 결과적으로 DDoS 공격에 대한 피해를 줄일수 있다. 본 논문에서 제안한 기법은 네트워크로 유입되는 패킷에 대하여 IP 주소를 수정하고 다시 전송하는 과정에서 전체적인 오버헤드가 증가 할 것으로 예상된다. 향후 네트워크에 부과되는 오버헤드를 최소화 하고, 네트워크로 유입되는 스캐닝 패킷을 감소시킬 수 있는 방안에 대한 연구가 필요하다.

참고문헌

[1] 홍성철, “엔터프라이즈 네트워크에서의 인터넷 웜 탐지를 위한 방법” KNOM Review Vol. 7, No. 2, December 2004

[2] 전용희 "인터넷 웜의 탐지 및 대응기술" 한국통신학회, 2005.08

[3] 신승원, “인터넷 웜 공격 탐지 방법 동향”, 한국전자통신연구원, 2005.02

[4] 권오철, “행동기반 탐지를 우회하는 웜 자기방어 기법안”, 한국정보과학회 가을 학술발표논문집, 2007

[5] Jelena Mirkovic, "A Taxonomy of DDoS Attack and DDoS Devense Mechanisms" ACM SIGCOMM Computer Communications Review, 2004

[6] 김용석, “우회 DoS 공격을 탐지하기 위한 모델 설계”, 한국정보과학회 추계학술대회, 2003

[7] 조유혁, “인터넷 서비스거부공격 유형분석” KTR&DZINE 2006.11