액티브 네트워크 기반의 분산 서비스 공격 대응 방안

Applied Research of Active Network to DDoS Attack

이성현, 이원구, 이재광*
한남대학교*

Lee seoung-hyun, Lee won-gu, Lee jae-kwang*
Hannam Univ*

요약

최근 인터넷을 통한 정보 전달이 생활화되고 있다. 또한 인터넷에서의 자료교환에 대한 증가로 인해 다른 사용자와 접속하기 위한 방식은 빠르게 변화하고 있다. 그러나 기존의 침입 차단 시스템과 침입 탐지 시스템과 같은 시스템 외부방어 개념의 보안 대책은 전산망 내의 중요한 정보 및 자원을 보호함에 있어서 그 한계를 갖는다. 본 논문에서는 분산 서비스 거부 공격에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 분석 및 설계한다.

Abstract

Recently, distributing information on the Internet is common in our daily life. Also, data exchange on Internet has rapidly changed the way we connect with other people. But current firewall and IDS(Intrusion Detection System) of the network level suffers from many vulnerabilities in internal computing informations and resources. In this paper, we analyzes Traceback System that based on active network and design of Traceback System that based on active network for efficiently traceback.

I. 서 론[1)]

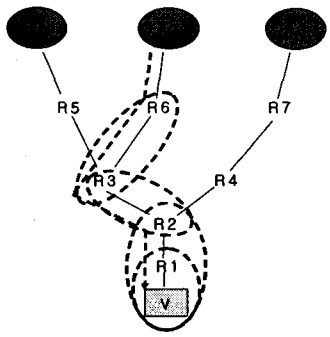
최근 컴퓨터 기술의 발달과 인터넷의 발전은 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 가져온 반면, 인터넷의 확장으로 인하여 외부의 시스템 불법 침입, 중요 정보의 유출 및 서비스 거부 공격 등의 역기능들이 계속해서 증가되어 그 피해가 심각한 수준이다.

최근의 정보보호 환경에서는 자신의 관리 도메인 내로 침입하게 되는 공격을 어떻게 잘 탐지 할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어 있다. 하지만 탐지된 침입의 공격자에 대한 대응도 자신의 도메인 경계에서 해당 트래픽을 차단하는 수동적인 방법 이외에는 별다른 방법이 없는 상태이고, 이 경우 자신의 도메인에서 파악한 침입자 정보를 바탕으로 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 자유로이 인터넷을 이용할 수 있을 뿐만 아니라 다른 공격 기술이나 공격 루트를 이용한 제2, 제3의 공격이 이루어 질 수 있다. 반면 인터넷을 이용한 경제 활동 및 그 액수가 점차 증가함에 따라 사이버 공격으로 입게 되는 피해는 점차 기업의 생존을 위협하는 수준에 도달하고 있다. 따라서 해킹에 능동적으로 대응할 수 있는 기술이 요구된다고 할 수 있으며, 능동적인 해킹 방어를 위한 가장 기본적인 기술로 해커의 실제 위치를 추적하는 역추적 기술을 활용할 수 있어야 한다. 그러나 현재까지 제안된 역추적 기술들은 인터넷이 보유한 다양성

1) 본 연구는 한국과학재단 목적기초연구 (R01-2002-000-00127-0)지원으로 수행되었음.

을 극복하지 못하여 현재의 인터넷 환경에 적용하는 데 어려움이 따른다[1].

이에 본 논문에서는 분산 서비스 거부 공격에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 설계한다. 2장에서는 분산 서비스 거부 공격과 역추적 기법을 살펴보고, 3장에서는 액티브 네트워크와 IDIP, AN-IDR에 대해서 분석하였으며 4장에서는 액티브 네트워크 기술을 이용한 역추적 방법을 제시하고 5장에서는 결론을 맺고 향후 연구방향을 기술하였다.



▶▶ 그림 1. 패킷의 전송경로와 공격경로

Ⅱ. 관련연구

2.1 분산 서비스 거부 공격

해킹 사건에 사용된 수법인 분산 서비스 거부공격(DDoS: Distributed Denial of service)은 마스터 서버에 접속하여 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부 공격을 수행하게 된다. 이럴 경우 트리누 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격하도록 하부 서버와 통신한다. 이는 공격자의 명령에 의해 공격 도구가 설치된 대량의 서버들을 제어해 공격 대상 시스템에 치명적인 서비스 거부 공격을 수행하기 때문에 인터넷을 교란시키려는 해커들에 의해 악용될 수 있다. 분산 서비스 거부 공격은 IP 패킷에 근원지 IP 주소를 스푸핑하여 공격하기 때문에 아래 그림 1과 같이 공격경로와 패킷의 경로는 서로 다르다는 것을 알 수 있다[2].

2.2 IP 역추적

대부분의 DDoS 공격은 해커의 위치를 숨기기 위해서 IP 주소를 변경하여 공격을 시도한다. 이러한 공격에 대응하기 위해서는 우선적으로 해커의 실제 위치를 찾아 대응하는 방법이 필요하며, 이를 위해서 해커의 공격 패킷으로부터 별도의 부가적인 정보를 수집하여 공격 패킷의 실제적인 주소를 찾는 것을 IP 역추적 기술이라 불리며 4가지 기법이 존재한다. 먼저 역추적 마킹 기법(Traceback Marking)기법으로 이는 패킷이 라우터를 거쳐갈 때, 라우터에서 자신의 특정 정보를 덧붙이고, 피해 시스템은 라우터 정보가 포함된 수신 패킷들을 통해 역추적하는 기법이다. 두 번째로 역추적 로깅 기법(Traceback Logging)기법은 라우터로 하여금 일정기간 동안 키 라우터를 거쳐가는 모든 패킷 정보를 기록하여, 데이터 마이닝 기법을 이용하여 패킷을 역추적하는 기법이다. 세 번째는 링트 테스팅(Link Testing)기법으로 공격이 이루어지고 있는 동안 피해 시스템에 가장 가까운 라우터에서 시작하여 전달되는 패킷의 위치를 거슬러 올라가는 기법이다. 마지막으로 ICMP 역추적 기법(ICMP Traceback)은 라우터에 거쳐 가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하여 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다[3].

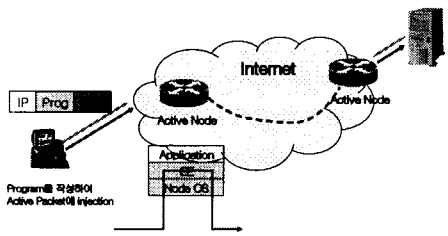
Ⅲ. 액티브 네트워크

1. 액티브 네트워크(Active Network)

사용자의 네트워크 요구 기능을 수행하기 위해 프로그램 코드를 전송 및 실행함으로써 통신망에 새로운 서비스를 신속하고 경제적으로 도입하고 망 자원들을 보다 적절하게 활용할 수 있도록 하는데 목표를 두고 연구되고 있는 분야가 액티브 네트워크 분야이다. 기존의 네트워크는 이를 이용하는 응용 및 사용자가 네트워크 환경에 스스로 적응하게 하면서 서비스를 제공하는 것과는 달리 액티브 네트워크는 사용자의 요구에 맞추어 서비스를 제공한다.

이러한 액티브 네트워크 운영 환경은 기존의 네트워크 노드가 단순히 패킷을 저장한 후 포워딩(store and forward) 하는 식의 단순한 네트워킹 기능을 하는 것과는 달리 액티브 네트워크는 사용자가 원하는 프로그램을 패킷을 통하여 전송하여 실행하거나 네트워크 노드에 미리 설치된 프로그램 중에서 해당 기능을 실행(store-compute-forward)함으로써 사용자가 원하는 네트워크 기능을 이용하게 된다.

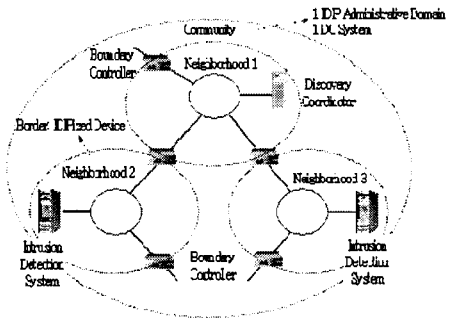
이처럼 네트워크 노드에서 라우팅과 같은 단순한 기능에서 벗어나 네트워크 종단간에서만 이루어지던 여러 가지 에러 처리 및 흐름 제어와 같은 복잡한 기능 혹은 그 외 사용자가 원하는 기능을 네트워크 노드에서 수행할 수 있다는 것은 사용자나 네트워크 망 자체에 유연성뿐 아니라 여러 많은 장점들을 제공할 수 있다[4].



▶▶ 그림 2. 액티브 네트워크 운영환경의 예

2. IDIP(Intruder Detection and Isolation Protocol) 분석

IDIP는 침입탐지 시스템, 방화벽, 호스트, 보안관리 관련 요소 시스템들 간의 협력 작업하기 위한 프로토콜을 포함한 보안 기반 구조이다. IDIP의 네트워크 구조는 DC(Discovery Coordinator) 시스템이 해당 도메인의 전체 IDIP 기능을 조율하고 관할하게 되는 'community'와, 그 경계를 IDIP가 실장된 시스템으로 이루어지는 'neighborhood'로 이루어진다. 하나의 'community' 내에는 하나의 DC 시스템만이 존재하고, 이 DC 시스템이 해당 'community' 내의 IDIP 기능을 제어, 관할하게 된다. 따라서 'community'는 하나의 독립된 IDIP 관리 영역으로 볼 수 있다. 'neighborhood'는 그 경계 안에 IDIP가 설정된 시스템이 존재하지 않는 경우로 IDIP를 구성하는 가장 기초적인 네트워크 요소로 볼 수 있다.

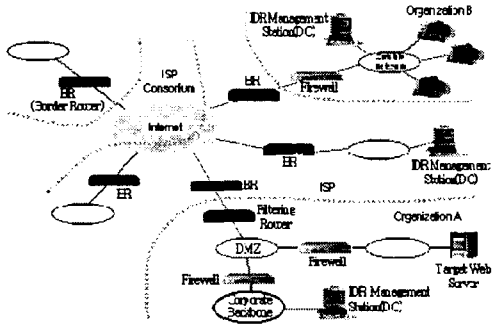


▶▶ 그림 3. IDIP에서의 네트워크 구조

3. AN-IDR(Active Network-Intrusion Detection and Response) 분석

AN-IDR의 구조는 기존 IDIP의 구조를 그대로 적용하고 있다. AN-IDR 구조에서 드러나는 변화는 AN-IDR의 보안상 관리 도메인을 계층적 구조로 가져가고 있다는 점이다. 이는 현실적으로 침입자를 추적하고 대응하기 위해서는 여러 관리 도메인을 지나 정보를 교환하거나 특정 시스템을 제어할 필요가 있는데, 각 망 사업자나 네트워크 서비스 제공 사업자

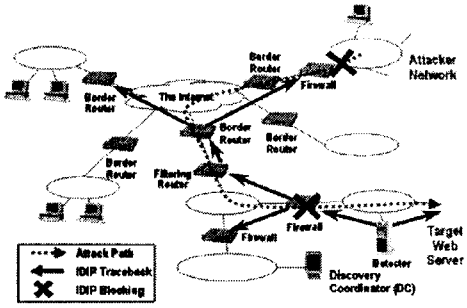
들이 자신의 망을 다른 사업자에게 제어권을 넘기지 않을 것에 대한 방안으로 고안된 것으로 보인다. 즉, 실제 필드에서 적용하기 위해 각 사업자는 자신이 관리하는 도메인에 대한 AN-IDR 관리 및 제어를 수행하고, 각 사업자들이 자신의 도메인에서 수행한 대응 방법을 조율하며, 정보를 공유하기 위해서 상위계층을 도입함으로써 각 사업자의 고유 권한을 침해하지 않으면서도 전체 AN-IDR의 기능을 수행할 수 있게 된다.



▶▶ 그림 4. AN-IDR의 네트워크 구조

Ⅳ. 액티브 네트워크기반의 침입자 역추적

액티브네트워크 기반의 역추적 시스템에서 만약 침입이 발생할 경우 먼저 침입탐지시스템이 공격이 발생하였음을 인접 IDIP 노드에게 알리고 공격자의 위치에 대한 역추적을 요청하게 된다. 이때 역추적을 요청하는 것과 동시에 동일 IDIP 노드들에게 대응을 요청하게 된다. 여기에서의 대응이란 해당 도메인의 보안 정책에 따라 해당 도메인에서 수행할 수 있는 대응 방법이 그 후보가 된다. 역추적 요청을 받게 되면 자신이 해당 공격과 관련된 패킷을 라우팅하였는지(혹은 호스트의 경우 해당 공격과 관련된 TCP 연결이 자신을 경유하여 나갔는지)를 판단하여 그 결과를 DC에게 보고한다. 만약 자신이 공격 경로 상에 존재한다면 자신의 인접 IDIP 노드(피해 시스템 방향은 제외한)에게 공격자에 대한 역추적을 계속 수행해 주도록 요청하게 된다. 만약 자신이 대응 시스템인 경우 해당 도메인의 보안 정책에 따라 임시적으로 해당 공격에 대한 대응을 수행하고 그 수행 결과를 DC에게 보고한다. 이런 역추적 요청의 일련 과정을 공격자의 실제 위치가 파악될 때까지 반복하여 공격자 경로 상의 IDIP 노드들이 수행하게 된다.



▶▶ 그림 5. 추적 결과 및 로컬 대응 결과 보고

Ⅴ. 결 론

방대한 네트워크 인프라의 확보와 이를 바탕으로 한 폭발적인 인터넷 사용자의 증가는 실제 물리적 공간에서의 세상과는 전혀 다른 인터넷이라는 사이버 공간을 창출하게 되었고, 이러한 사이버 공간에서는 전 세계의 현실공간의 모든 정보가 생성 및 저장, 유통됨으로써 실생활에서 수행할 수 있는 대부분의 일들을 온라인 상에서 진행할 수 있게 되었다. 그러나, 이러한 정보화 사회는 긍정적인 측면이 있는 반면에 부정적인 측면도 대두되게 되었다[5]. 특히 부정적인 측면은 개인 생활의 파멸을 초래할 수도 있을 뿐만 아니라, 국가적인 안보의 위협까지 초래할 수 있다. 대표적인 부정적 측면은 인터넷을 통한 해킹, 악성 웜과바이러스의 유포, 지적 재산권의 침해, 사이버 범죄에의 이용, 대규모 네트워크에 대한 가용성 고갈 등을 열거할 수 있으며, 이는 최근 발생한 "1.25 인터넷 대란"을 보면 쉽게 알 수 있다. 따라서 본 논문에서는 이러한 침입에 대한 대응을 위해 액티브 네트워

크기반의 역추적 시스템을 분석 및 설계하였다.

향후 연구로는 액티브 네트워크 기술을 이용한 역추적 기법이 실제 적용되도록 하기 위해서 하부 플랫폼에 독립적인 실행 환경을 갖고 이동형 실행 패킷(액티브 패킷)을 적용함으로써 유연성, 확장성을 가지는 능동적인 역추적 시스템에 대한 연구가 이루어져야 할 것이다.

▌참고문헌▐

[1] 이만영, 손승원, 조현숙, 정태명, 채기준 "차세대 네트워크 보안 기술" 생능출판사, pp.415-430, 2002.11.25

[2] 이형우, "DDoS 해킹 공격 근원지 역추적 기술" 정보보호학회지, 2003.10.

[3] 강호호외 3명, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원.

[4] "차세대 인터넷을 위한 능동 보안 기술백서", 한국전자통신연구원, 2001.5.15.

[5] 정종민, 이지율, 이구연, "다중 에이전트를 이용한 역추적 시스템 설계 및 구현", 한국정보보호학회 논문지, 제13권 4호, pp.3~11, 2003.8.

[6] Chun He, Formal Specifications of Traceback Marking Protocols, June 14, 2002.

[7] S. Savage, D. Wetherall, A. karlin, and T. Anderson, Network Support for IP Traceback, IEEE/ACM transactions on networking, vol. 9, No. 3, June 2001.