IP 역추적 시스템 분석 및 설계

Analysis and Design of IP Traceback System

황영철, 최병선, 이성현, 이원구, 이재광*
한남대학교*

Hwang yonung-chul, Choi byoung-son,
Lee seoung-hyeon, Lee won-gu, Lee jae-kwang*
Hannam Univ*

요약

컴퓨터와 네트워크의 보급이 일반화 되면서 인터넷을 통한 정보 전달이 일상 생활처럼 되고 있다. 또한 인터넷, 무선통신, 그리고 자료 교환에 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 해킹으로 판단되는 침입에 대하여 라우터의 구조적 변경 없이 효율적으로 역추적 하기 위해서 ICMP 역추적 메시지(ICMP Traceback Message)를 이용한 ICMP 기반의 역추적 시스템을 설계한다.

Abstract

As computers and networks become popular, distributing information on the Internet is common in our daily life. Also, the explosion of the Internet, of wireless digital communication and 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 design of ICMP-based Traceback System using a ICMP Traceback Message for efficiently traceback without change structure of routers. ICMP-based Traceback System.

I. 서 론[1)]

최근 정보통신 기술과 정보 시스템이 급속한 속도로 발전한 것에 비례하여, 정보시스템 보안 대책도 동시에 발전하고 있다. 그러나 우리나라의 경우, 아직도 대부분의 사용자가 시스템 보안에는 무관심한 것이 사실이다. 따라서, 이에 대한 개개인의 자각과 더불어 효율적인 보안이 요구되게 되었다. 세계 각국이 정부를 중심으로 보안에 대한 연구를 주도하여, 각 연구소와 대학에서 보안에 대한 연구를 진행하고 있다. 현재 연구중인 대표적인 보안 기술로는 역추적 시스템 있다. 그러나 현재까지 제안된 역추적 기술들은 인터넷이 보유한 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다. 따라서 본 논문에서는 능동적인 해킹 방어를 위한 역추적 시스템을 분석하고, 침입 대응을 위해 ICMP 기반의 효율적인 역추적 시스템을 설계하였다[1].

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

Ⅱ. 관련연구

대표적으로 연구 중인 IP 역추적 기술로는 IP 패킷 마킹(IP Packet Marking) 기술이 있다. IP 패킷 마킹 기법은 패킷이 전송되는 동안 라우터에서 패킷에 확률적으로 경로정보를 마킹하는 방법이다. 지금까지 IP 기반의 패킷 마킹 기술의 흐름은 DDoS공격에 대한 해결책으로서 많이 연구되고 있다. 공격자는 여러 명이 될 수도 있으며, 수많은 패킷을 생성하여 전송할 수 있다. 이 기법은 네트워크에서 패킷이 전송되는 동안 부분적인 경로 정보를 가지고 라우터에서 확률적으로 패킷에 마킹을 하게 된다. 이렇게 마킹된 패킷을 받은 피해 호스트는 마킹된 패킷을 이용하여 공격자의 근원지를 네트워크 상에서 찾아가게 되는 기법이다. 하지만 이러한 마킹 기술들은 라우터가 해당 패킷에 대해서 마킹을 한 후, 다음 노드로 전송해야 하기 때문에 라우터의 과부하 문제가 발생할 수 있으며 하나의 패킷에 마킹될 필드에 대한 공간 문제가 발생 할 수 있다. 또한 단편화(Fragmentation) 문제를 유발할 수 있다. 이와 같이 현재의 역추적 방식의 문제점을 해결하여 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 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다[2][3].

1. 호스트 기반 역추적 시스템

1.1 CIS(Caller Identification System)

CIS(Caller Identification System)는 H.T. Jung에 의해 1993년 제안된 시스템이다. 이 역추적 시스템은 실제 역추적이라기 보다는 미리 사용자가 거쳐 온 시스템의 목록을 관리하는 것으로, 정상적인 사용자들이 접속하는 데도 많은 지연을 초래하게 된다. 또한 침입이 발생하기 이전에 수행하는 작업이 많기 때문에, 자원 활용 면에서 비효율적이라고 할 수 있다. 그리고, CIS는 접속을 원하는 사용자가 거쳐 온 시스템 각각에 대한 인증을 거쳐 가는 시스템마다 요구하므로 이로 인한 네트워크 부하가 크고, CIS에 오고 가는 인증을 위한 메시지의 무결성을 보장하지 못하는 단점이 있다[2].

2. 네트워크 기반 연결 역추적 시스템

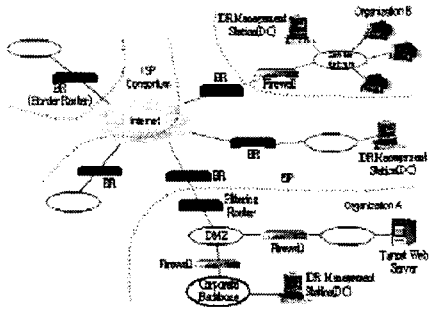
2.1 SWT(Sleepy Watermark Tracing)

Sleepy watermark 역추적 시스템은 침입에 대한 응답 패킷에 워터마크를 삽입하여 역추적을 수행한다. SWT 기법은 다음과 같은 형태로 이루어진다. 한 네트워크에는 guardian gateway가 존재하고, 이와 연동되어 동작하는 guarded host가 존재한다. 최초 침입이 발생할 때까지는 아무런 추가적인 동작이 진행되지 않은 일반적인 상태로 존재한다. 침입이 발생되면 이는 guarded host내의 IDS에 의해 탐지된다. guarded host의 SWT subsystem의 sleepy intrusion response 모듈의 작동이 시작되고 이때부터 일반 host에 도착되는 패킷에 의한 응답은 watermark enabled application에 의해 작성되기 시작한다. 이는 일반적인 응답패킷에 워터마크를 삽입하여 송신을 시작한다. 이렇게 역추적이 시작되면 이는 guardian gateway의 active tracing 모듈과 연동되어 워터마크가 삽입된 패킷을 찾기 시작한다. 본 SWT 역추적 기법은 공격에 대한 응답 패킷을 이용하여 해커의 위치를 추적하기 때문에 빠르고 정확한 역추적이 가능하다. 그러나, watermark enabled application이 필요하다는 문제로 인해 실제 인터넷 환경에 적용하기에는 큰 문제를 가지고 있다. 또한 해커에 의해 사용되는 연결이 암호화 되는 경우에는 역추적이 전혀 불가능할 수 있다는 단점이 존재한다[3].

3. AN-IDR

AN-IDR(Active Network-Intrusion Detection

and Response)의 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 사업자들이 자신의 망을 다른 사업자에게 제어권을 넘기지 않을 것에 대한 방안으로써 고안된 것으로 보인다. 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 상위 계층을 도입함으로써 각 사업자의 고유 권한을 침해하지 않으면서도 전체 AN-IDR의 기능을 수행할 수 있게 된다[4].



▶▶ 그림 1. AN-IDR의 네트워크 구조

4. ICMP 기반 역추적 시스템

ICMP 기반 역추적 시스템에서는 역추적을 위해 IETF Internet Area의 itrace Working Group에서 표준화 중인 ICMP Traceback Message를 이용하여 역추적을 진행한다. 해당 기술은 수사적 관점에서 해커의 위치를 보다 정확하고 신속하게 파악하고자 하는 공공기관에 적용 할 수 있으며, 기업체 및 공공기관 내부망에 설치하여 내부망 내의 최초 공격 지점을 찾아 내부망 보호를 위한 기술로 활용할 수 있다[5].

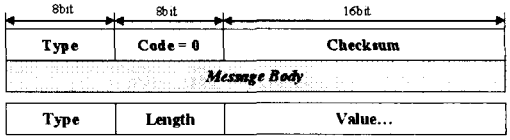
Ⅲ. ICMP 기반의 역추적 시스템 설계

1. ICMP Trace 기법

ICMP 역추적 기법은 라우터에 거쳐 가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하고 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다.

2. ICMP 역추적 메시지

ICMP 역추적 메시지(ICMP Traceback Message)는 현재 IETF internet Area의 itrace Working Group에서 Internet draft로 제출된 상태이다. ICMP 역추적 메시지는 ICMP 패킷의 Message Body에 일련의 스트링으로 포함된다. ICMP Traceback Message를 위한 ICMP Type은 현재 정의되지 않았지만, IANA에서 조만간 정의 할 예정이다. Code 필드는 항상 '0'으로 설정되며, Message Body는 하나의 이상의 TLV (Type-Length-Value) 엔트리로 구성된다. [그림 2]는 ICMP 역추적 메시지 형태를 보여주고 있다.



▶▶ 그림 2. ICMP Traceback Message 형태

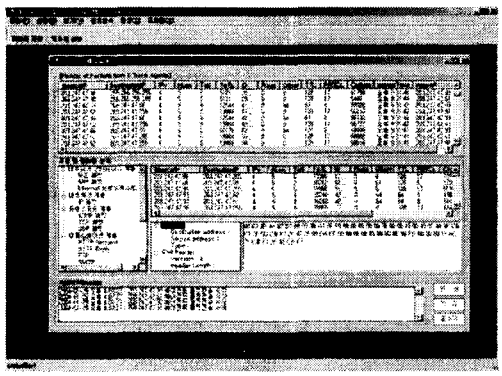
최상의 TVL 엔트리는 0개 이상의 서브 TVL 엔트리를 가지며, 서브 TVL엔트리는 최상의 TVL 엔트리의 Value에 포함된다. Type의 범위는 0x01~0x08 이다[5][6].

Ⅳ. 임계치 설정 및 패킷 모니터링

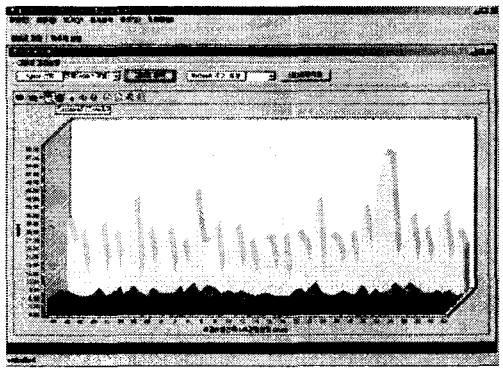
설정 임계치에 따라 패킷 모니터링을 통한 패킷 캡쳐를 제공하며, 패킷 헤더 정보를 ICMP 메시지 생성 모듈에 전달한다.

▶▶ 그림 3. 임계치 설정 화면

ICMP 생성 모듈은 ICMP 헤더를 작성하고, 작성된 ICMP 헤더 정보를 전송모듈에 전달하여 생성된 ICMP 메시지를 역추적 매니저에게 전달한다.



▶▶ 그림 4. I-Trace Manager 패킷 모니터링



▶▶ 그림 5. I-Trace Manager 패킷 모니터링(그래프)

V. 결 론

인터넷 사용자의 급속한 증가로 인한 복잡한 TCP 반응과 연관되어 네트워크 서비스에 많은 패킷 손실을 야기하게 되었다. 이러한 문제를 해결하기 위하여 대학 연구소와 기업체에서는 침입대응 시스템을 개발하게 되었고, 공격자의 근원지를 추적하는 역추적 시스템이 등장하게 되었다. 따라서 본 논문에서는 이러한 침입에 대한 대응을 위해 ICMP 기반의 역추적 시스템을 분석 및 설계하였다. 향후 연구로는 세밀한 분석을 통하여 모듈을 설계하고, 이 설계를 바탕으로 역추적 Agent와 역추적 Manager를 구현하고자 한다. ICMP 역추적 메시지는 현재 IETF internet Area의 itrace Working Group에서 Internet draft로 제출된 상태이다[5]. ICMP 역추적 기법은 라우터에 거쳐 가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하고 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다. 더 나아가 이를 능동 네트워크 기반으로 발전시켜 새로운 역추적 시스템을 구현하고자 한다.

▌참고문헌▐

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

[2] 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.

[3] D. Song and A. Perrig, Advanced and authenticated marking schemes for IP Traceback, in Proc. IEEE INFOCOM, vol. 2, April 2001, pp.878-886.

[4] Dan Sterne, "Active Network Intrusion Detection and response (AN-IDR)", Boeing and NAI LAB., DARPA FTN PI Meeting, Jul. 20, 2000.

[5] Allison Mankin외 4명, "On Design and Evaluation of Intention-Driven ICMP Traceback"

[6] Steve Bellovin외 2명, "ICMP Traceback Messages", Internet Draft, IETF, Feb. 2003.