리눅스 기반의 IP 역추적 시스템 분석 및 설계

이원구*, 이재광*
*한남대학교 컴퓨터공학과

Analysis and Design of Linux-based IP Traceback

Won-Goo Lee*, Jae-kwang Lee*
Dept. of Computer Engineering, Hannam University*

요 약

인터넷 사용자의 급증에 따라, 인터넷을 통한 다양한 해킹 및 불순한 의도를 지닌 공격에 의한 침해사고 역시 크게 증가되고 있다. 이러한 해킹의 피해로부터 네트워크 시스템 및 서버를 보호하기 위해 각종 보안 강화 시스템이 개발되어 운용되고 있으나, 현재 사용 중인 보안강화 도구들은 수동적인 방어 위주로 공격자의 해킹 시도 자체를 제한하는 것이 아니라 해킹이 시도된 후 대처하는 제약 등으로 해킹 자체를 방지하는 데는 한계를 가지고 있다. 능동적인 해킹 방어를 위한 가장 기본적인 기술은 해커의 실제 위치를 추적하는 역추적 시스템이라 할 수 있다. 현재 이에 대한 연구가 활발히 진행 중에 있다. 따라서 본 논문에서는 능동적인 해킹 방어를 위한 역추적 시스템을 분석하고, 리눅스 기반의 역추적 시스템을 설계하였다.

1. 서론

최근 인터넷의 급속한 보급 확대 및 대중화에 따라 네트워크상의 서비스 속도와 정보보안은 인터넷 사용자에게 중요한 문제로 대두되고 있고, 이로 인해 네트워크의 트래픽 증가와 공격자로부터의 공격이 점점 증가하고 있는 현실이다. 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[1].

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 마킹 될 필드에 대한 공간 문제가 발생 할 수 있다. 또한 단편화(Fragmentation) 문제를 유발할 수 있다[2].

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.

이에 본 논문에서는 해킹으로 판단되는 침입에 대하여 라우터의 구조적 변경 없이 효율적으로 역추적하기 위해서 ICMP 역추적 메시지(ICMP Traceback Message)를 이용한 ICMP 기반의 역추적 시스템을 설계한다. 2장에서는 역추적 시스템을 동향을 분석하여 보고, 3장에서는 ICMP의 역추적 시스템을 설계하였으며 4장에서는 결론을 맺고 향후 연구방향을 기술하였다.

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

2. 관련연구

2.1 호스트 기반 역추적 시스템

2.1.1 CIS(Caller Identification System)

CIS(Caller Identification System)는 H.T. Jung에 의해 1993년 제안된 시스템이다. 이 역추적 시스템은 실제 역추적이라기 보다는 미리 사용자가 거쳐온 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 거쳐온 시스템 각각에 대한 인증을 거쳐가는 시스템마다 요구하므로 이로 인한 네트워크 부하가 크고, CIS에 오고 가는 인증을 위한 메시지의 무결성을 보장하지 못하는 단점이 있다[3].

2.1.2 AIAA

AIAA(Autonomous Intrusion Analysis Agent) 시스템은 침해를 당한 서버의 해킹 피해 분석과 추적을 위한 로그 분석을 에이전트를 이용해 자동화한 역추적 시스템이다. AIAA 시스템은 침입자가 거쳐온 경유 시스템의 관리자의 도움을 받아 AIAA를 설치하고, 이 시스템에서 바로 이전의 침입경로와 해킹 흔적을 분석하고 다시 이전의 침입시스템으로 분석을 옮겨가서 최종 경유지 서버까지 거슬러 간다.

본 시스템은 역추적 경로상에 존재하는 시스템들의 관리자의 도움을 받아 설치하기 때문에 역추적을 완료하기까지 많은 시간이 필요하게 된다. 또한 역추적 경로상에 존재하는 모든 시스템에 직접 접속해야 하기 때문에 만약 관리자와의 협조가 불가능하여 시스템으로의 접근이 불가능한 경우 역추적 자체가 불가능할 수도 있다[3].

2.2 네트워크 기반 연결 역추적 시스템

2.2.1 Thumbprints based algorithm

Thumbprint란 말 그대로 지문을 의미한다. Thumbprint를 이용하는 방법은 역추적 시스템 전체를 의미하는 것이 아니라 역추적을 위해 공격자의 시스템으로부터 공격 대상 시스템까지의 연결 체인을 구성하는 알고리듬이다. 본 알고리듬은 연결 체인에 속하는 호스트들이 속한 네트워크 상에 송수신되는 데이터를 수집하여 비교한다. 그러나 패킷이 암호화되거나 터널링되어 패킷의 내용이 변경되는 경우, 해당 연결 체인을 구성할 수 없는 경우가 발생할 수 있다[4].

2..2.2 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[5][6].

2.3 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 내부망내의 최초 공격 지점을 찾아 내부망 보호를 위한 기술로 활용할 수 있다[7][8].

표 2. 역추적 시스템 분석 및 비교

방식	장점	단점
ICMP 기반	-역추적 성공률이 높다 -암호화되거나 스푸핑된 패킷에 대해 역추적 가능 -IETF 표준화 진행중 (ICMP Traceback Message)	- 에이전트 문제
수동 역추적 기술	- 신뢰성 보장	-시간 소용가 많음
CIS를 이용한 역추적	- 특정 도메인내에서 빠른 역추적 가능	- 비표준화, 비현실성
Tumbprint를 이용한 역추적	- 정확한 Tumbprint만 있으면 바른 역추적 가능	- Tumbprint 값의 동기화와 시스템 시간의 정확성을 요구

3. 역추적 시스템 모듈 설계

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 설계하였다. ICMP 역추적 메시지의 생성은 라우터를 포트 미러링하는 "역추적 Agent"가 담당하며, 이 메시지를 수신하는 피해 시스템은 해당 메시지를 저장하고, "역추적 Manager"가 DDoS류 공격을 탐지하게 되면 해당 메시지 정보를 이용하여 역추적을 시작한다.

3.1 역추적(IP Traceback) 시스템

현재의 인터넷 환경에 적용하여 사용할 수 있는 새로운 역추적 시스템은 기존의 역추적 시스템들과는 달리 비록 모든 중간 경유지를 확인할 수 없다하더라도 해커의 최종 위치를 찾을 가능성을 최대화 한다는 점에서 장점을 지닌다고 할 수 있다. 그림 1은 ICMP 기반의 역추적 시스템의 전체 구성도를 보여주고 있다.

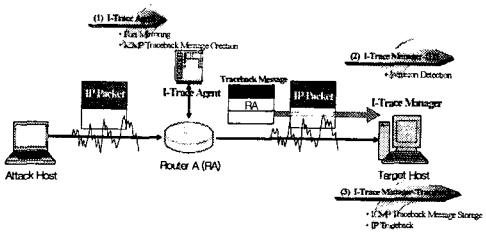

그림 1. ICMP 기반의 역추적시스템의 전체구성도

역추적 에이전트는 지속적으로 라우터에 대해서 포트 미러링을 수행하면서 확률적 근거에 의해서 ICMP 역추적 메시지를 생성하여 대상 호스트에 전달한다. 침입탐지 기능을 가지고 있는 역추적 manager가 설치된 대상 호스트는 DDoS류 공격에 대해서 공격을 탐지하면 그 동안 수집된 ICMP 역추적 메시지들을 이용하여 역추적을 수행하게 된다. 이러한 역추적을 수행하기 위해서는 다음과 같은 구성이 필요하다.

(1) 역추적 Agent
  ① 역추적 에이전트에 의한 포트 미러링
  ② 역추적 검출 확률 설정에 의한 ICMP 메시지 생성 및 Target 호스트 주소로 전송

(2) 역추적 Manager (침입 탐지 기능)
  ① 임계치(threshold)에 근거한 DDoS공격 탐지

(3) 역추적 Manager (역추적 기능)
  ① ICMP 역추적 메시지에 대한 데이터 마이닝을 통한 공격 경로 추적 및 근원지 확인

3.2 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, 공격이검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다.

3.3 ICMP 역추적 메시지(ICMP Traceback Message)

ICMP 역추적 메시지는 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. 아래 그림 2는 ICMP 역추적 메시지 형태를 보여주고 있다.

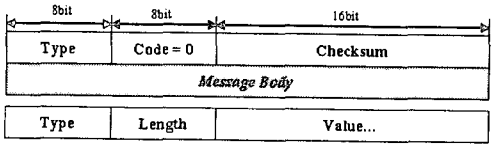

그림 2 ICMP Traceback Message 형태

최상의 TVL 엔트리는 0개 이상의 서브 TVL 엔트리를 가지며, 서브 TVL엔트리는 최상의 TVL 엔트리의 Value에 포함된다. Type의 범위는 0x01~0x08이다. 표 2는 최상의 TVL 엔트리를 보여주고 있다.

표 3 최상의 TVL

Type	Element Name
0×01	Back Link
0×02	Forward Link
0×03	Timestamp
0×04	Traced Packet Contents
0×05	Probability
0×06	RouterId
0×07	HMAC Authentication Data
0×08	Key Disclosure List

4. 임계치 설정 및 패킷 모니터링

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

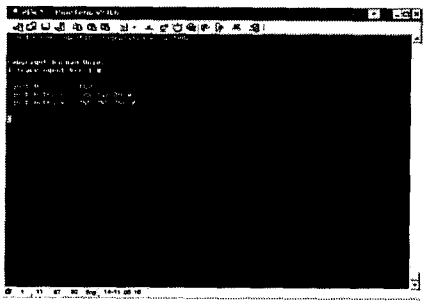

그림 3 임계치 설정 화면

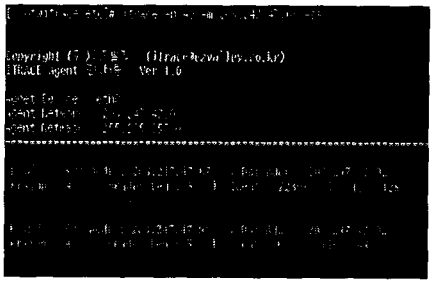

그림 4 역추적 Agent의 패킷 모니터링

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

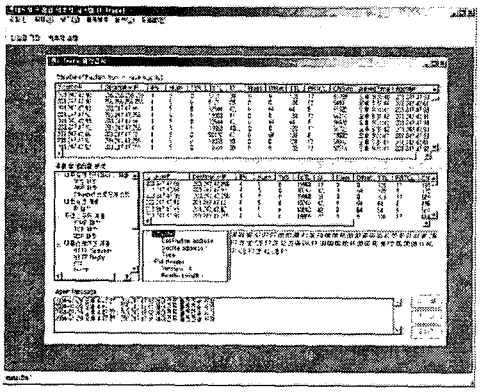

그림 5 역추적 Manager 패킷 모니터링

5. 결론 및 향후 연구

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[1]. 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 ICMP 기반의 역추적 시스템을 분석 및 설계하였다. 향후 연구로는 세밀한 분석을 통하여 모듈을 설계하고, 이 설계를 바탕으로 역추적 Agent와 역추적 Manager를 구현하고자 한다.

[참고문헌]

[1] 강동호외 3명, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원

[2] 정종민, 이지율, 이구연, "다중 에이전트를 이용한 역추적 시스템 설계 및 구현", 한국정보호학회 논문지, 제 13권 4호, pp.3-11, 2003. 8

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

[4] 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.

[5] R. Stone, CenterTrack: An IP overlay network for tracing DoS floods , in Proc, 2000 USENIX Security Symp., July 2000, pp. 199-212.

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

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

[8] Steve Bellovin외 2명, "ICMP Traceback Messages", Internet Draft, IETF, February 2003