ICMP 역추적 메시지를 이용한 IP 역추적 시스템

채철주*, 최병선*, 이재광*
*한남대학교 컴퓨터공학과
e-mail:cjchae@netwk.hannam.ac.kr

The Design of IP Traceback System using ICMP Traceback Message

Cheol-Joo Chae*, Byung-Sun Choi*, Jae-Kwang Lee*
*Department of Computer Engineering, Hannam University

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 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.

1. 서론[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.

2. 관련연구

역추적이란 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기술을 말하는 것으로 해킹 공격 근원지를 검출하는 방법에 따라 전향적(proactive) 역추적 방법과 대응적(reactive) 역추적 방법으로 나눌 수 있다.[2]

2.1 전향적(proactive) 역추적 기술

전향적 역추적 기술이란 해킹 공격이 발생한 것이 확인되었다면 해킹 공격에 의한 연결이 형성되어 있는 상태에서 공격 근원지를 역추적 하는 방법이다. 이러한 전향적 역추적 기술은 패킷이 전송되는 과정에서 미리 역추적 경로 정보를 생성한 후 패킷에 삽입하거나 목적지로 전달하여 주기적으로 관리하여 해킹 공격이 발생하면 수집된 정보를 이용하여 공격 근원지를 식별한다.

2.1.1 Node Append 기법

마킹 기법중 가장 간단한 Node Append 기법은 공격자의 패킷이 네트워크를 지나갈 때 노드의 주소를 공격자의 패킷에 추가해서 이 주소를 이용하여

공격자의 위치를 역추적 하는 기법이다. 피해 호스트에서는 받은 모든 패킷은 지나온 경로를 순차적으로 가지고 있기 때문에 역추적 경로를 구성하는데 시간이 짧다. 하지만 라우터들의 오버헤드와 경로의 전체 길이를 알 수 없기 때문에 패킷 공간 확보의 어려움이 있고 공격자가 거짓된 정보로 공간을 채울 수도 있다.[3]

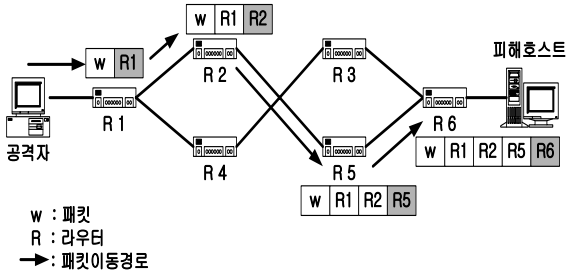

그림 1 Node Append 기법

2.1.2 Node Sampling 기법

Node Sampling 기법은 Node Append 기법의 단점인 라우터의 트래픽 증가와 패킷 공간 확보 문제를 해결하기 위해서 확률 p를 이용하여 경로 정보를 마킹하는 기법이다. 피해 호스트에서는 충분한 패킷을 받는다면 모든 라우터에 대한 경로 정보를 얻을 수 있지만 샘플의 수가 충분하지 못하다면 경로를 구성할 수 없다는 단점이 있다.[3]

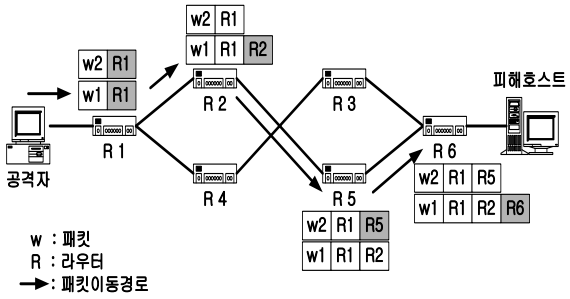

그림 2 Node Sampling 기법

2.1.3 Edge Sampling 기법

Edge Sampling 기법은 Node Append 기법과 Node Sampling 기법의 단점을 보완한 기법으로서 Edge 샘플의 거리를 표현하는 필드와 링크의 각 끝에 라우터의 IP 주소를 표현하기 위해 각 패킷에 고정된 start 주소 필드와 end 주소 필드를 예약한다. 마킹을 결정하면 start 필드에 라우터 자신의 주소를 마킹하고 거리 필드에 0을 기록한다. 만약 거리 필드에 0이 기록되어 있으면 거리 필드의 값을 1 증가한다.[3]

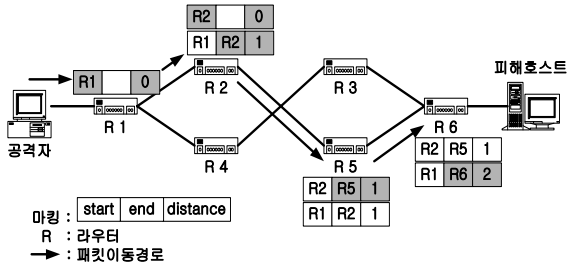

그림 3 Edge Sampling 기법

2.1.4 Messaging 기법

Messaging 기법은 라우터에서 다음 노드에 대한 정보를 담고 있는 메시지를 생성해서 전송하는 기법으로서 IETF가 제안한 ICMP 메시지 추적 기법이 대표적이다. ICMP 메시지 추적 기법에서 라우터는 ICMP 역추적 메시지를 생성하여 패킷의 목적지 주소에 메시지를 전송하고 중간 시스템은 해당 정보를 수집하여 공격이 검출되면 수집된 정보를 이용하여 역추적 하게 된다. 이는 공격 중에도 이 정보를 이용하여 추적이 가능하고 또한 공격이 종료된 후에도 추적이 가능하다는 장점이 있다.[4]

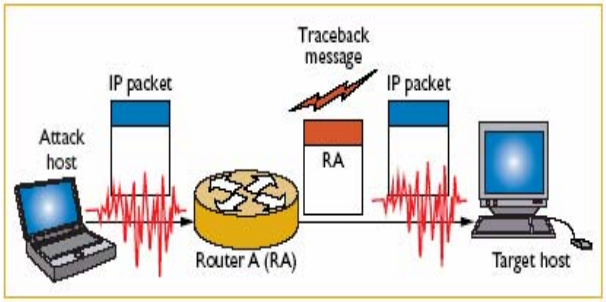

그림 4 Messaging 기법

2.1.5 Ingress filtering 기법

Ingress filtering은 다른 라우터로부터 비정상적인 소스 주소로부터 입력되는 패킷들을 차단하는 기법이다. 이는 라우터를 통과하는 모든 패킷에 대해서 소스 주소를 조사할 수 있는 능력이 있어야만 가능하다. Ingress filtering 기법은 오버헤드를 초래해 성능저하를 가져올 수 있으며 Ingress filtering을 지원하는 라우터가 널리 설치되어 있어야만 효과적이다.[4]

2.1.6 Logging 기법

핵심 라우터에서 포워드된 패킷 로그를 저장하고 데이터 마이닝 기법을 이용하여 패킷이 지나온 경로를 결정하는 기법으로 공격이 끝난 후에도 추적이 가능하다는 장점이 있지만 로그를 처리하기 위한 방

대한 자원이 필요하다는 단점과 방대한 로그 데이터 베이스를 통합할 때 ISP들 간의 충돌문제를 야기한다.

2.2 대응적(reactive) 역추적 기술

대응적 역추적 기술은 해킹 공격에 발생한 것을 확인한 후 해킹 공격에 의한 연결이 형성되어 있는 상태에서 공격 근원지를 역추적하는 방법이다. 대표적인 대응적 역추적 기술로는 오버레이 네트워크 기반 역추적 기법과 해쉬 기반 IP 역추적 기법이 있다.

오버레이 네트워크 기반 역추적 기법에서는 역추적 라우터 모듈을 네트워크에 별도로 설치하고 해킹 공격이 발생하였을 경우 네트워크의 종단 시스템과 연결된 라우터에서 전달된 정보를 역추적 라우터로 전송한다. 역추적 라우터에서 수집된 패킷 관련 정보를 재구성하여 실제로 패킷이 전달된 경로를 분석하는 방법이다.

해쉬 기반 IP 역추적 기법에서는 SPIE(source path isolation engine)기반 역추적 서버를 구성하고 전체 네트워크를 하위 그룹으로 나누어서 각 그룹별로 에이전트를 두어 망을 관리한다. 그리고 각 라우터에는 DGA(data generation agent) 기능을 탑재하여 운영하는데 DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬값에 대당하는 IP 헤더 정보와 8 바이트 정보의 payload 정보를 수집 관리하고 이를bloom filter 구조로 저장한다. 해킹 공격이 발생하였을 경우에는 네트워크 그룹을 관리하는 SCAR 에이전트를 통해 그룹내 DGA 라우터에 저장된 정보와 해킹 패킷 정보를 비교 분석하여 역추적 경로를 재구성한다.

3. ICMP Message를 이용한 역추적 시스템 설계

3.1 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, 공격이검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다. 이는 공격 중에도 이 정보를 이용하여 추적이 가능하고 또한 공격이 종료된 후에도 추적이 가능하다는 장점을 가지고 있다.

3.2 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 5은 ICMP 역추적 메시지 형태를 보여주고 있다.

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

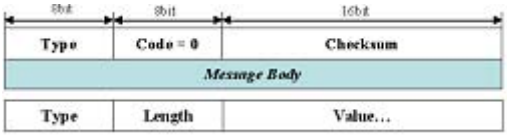

그림 5 ICMP Traceback Message 형태

4. 임계치 설정 및 패킷 모니터링

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

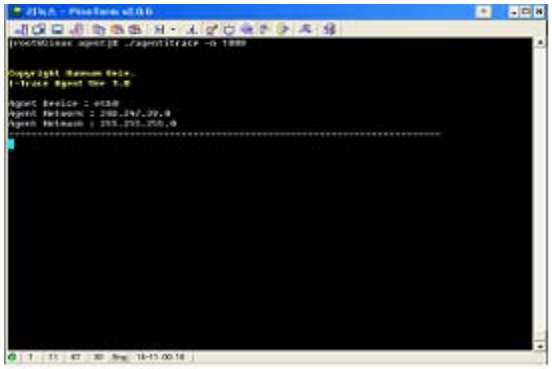

그림 6 임계치 설정 화면

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

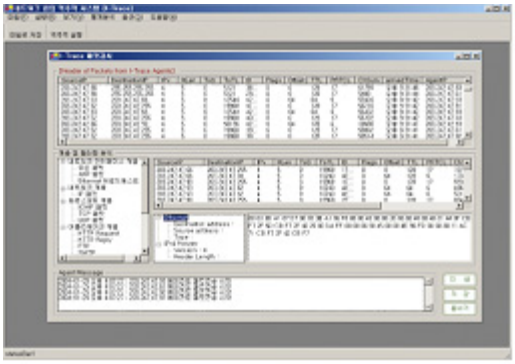

그림 7 I-Trace Manager 패킷 모니터링

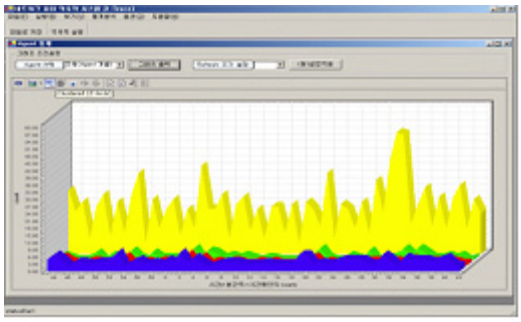

그림 8 I-Trace Manager 패킷 모니터링(그래프)

5. 결론

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. ICMP 역추적 기법은 라우터에 거쳐가는 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] Tatsuya Baba and Shigeyuki Matsuda, Tracing Network Attacks to Their Source, http://computer.org/internet/, 2002

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

[4] Tatsuya Baba and Shigeyuki Matsuda, Tracing Network Attacks to Their Source, http://computer.org/internet/, 2002

[5] 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.

[6] Allison Mankin외 4명, “On Design and Evaluation of Intention-Driven ICMP Traceback”

[7] Steve Bellovin외 2명, “ICMP Traceback Messages”, Internet Draft, IETF, February 2003

[8] “차세대 인터넷을 위한 능동 보안 기술 백서”, 한국전자통신연구원

[9] Steve Bellovin외 2명, “ICMP Traceback Messages”, Internet Draft, IETF, February 2003