네트워크 침입자 대응을 위한 ICMP 기반의 역추적 시스템

이직수, 이성현, 이재광

Traceback System based on ICMP for Network Intruder Response

Jik-Su Lee, Seoung-Hyeon Lee, Jae-kwang Lee

요 약

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. 따라서 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 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다. 이에 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.

Ⅰ. 서 론[1)]

컴퓨터 기술의 발달과 더불어 인터넷의 발전은 데이터 전송 속도의 과속화와 대용량의 데이터 전송 등의 기술을 증가시켜 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. 따라서 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 루트

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

를 이용한 제2, 제3의 공격이 이루어 질 수 있다. 반면 인터넷을 이용한 경제 활동 및 그 액수가 점차 증가함에 따라 사이버 공격으로 입게되는 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 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다[1].

이에 본 논문에서는 해킹으로 판단되는 침입에 대하여 효율적으로 역추적 하기 위해서 ICMP 기반의 역추적 시스템을 설계한다. 2장에서는 역추적 시스템을 동향을 분석하여 보고, 3장에서는 ICMP기반의 역추적 시스템을 설계하고 4장에서는 ICMP 기반의 역추적 시스템에서의 패킷 모니터링에 대해서 살펴보고 5장에서는 결론을 맺고 향후 연구방향을 기술하였다.

II. 관련연구

2.1 DDoS(Distributed Denial of Service)

해킹 사건에 사용된 수법인 분산 서비스 거부 공격(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 공격경로와 패킷의 경로는 서로 다르다.

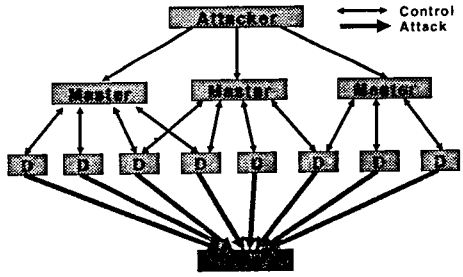

그림 1. DDoS 공격 구조

그림 2는 분산 서비스 공격의 경우 공격경로와 패킷의 경로가 서로 다르다는 것을 보여주고 있다[2].

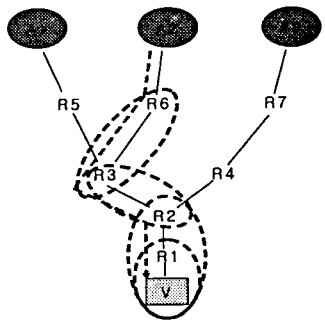

그림 2. 패킷의 전송경로와 공격경로

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 거쳐가는 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].

2.3 호스트 기반 역추적 시스템

2.3.1 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[4].

2.3.2 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[4].

2.4 네트워크 기반 역추적 시스템

2.4.1 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].

2.4.2 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].

III. ICMP 기반 역추적 시스템 설계

4.1 ICMP Trace 기법

ICMP 역추적 기법은 라우터에 거쳐 가는 패

킷에 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.

4.2 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 3은 ICMP 역추적 메시지 형태를 보여주고 있다.

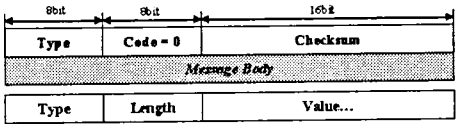

그림 3. ICMP Traceback Message 형태

최상의 TVL 엔트리는 0개 이상의 서브 TVL 엔트리를 가지며, 서브 TVL엔트리는 최상의 TVL 엔트리의 Value에 포함된다. Type의 범위는 0x01~0x08이다[7].

IV. 임계치 설정 및 패킷 모니터링

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

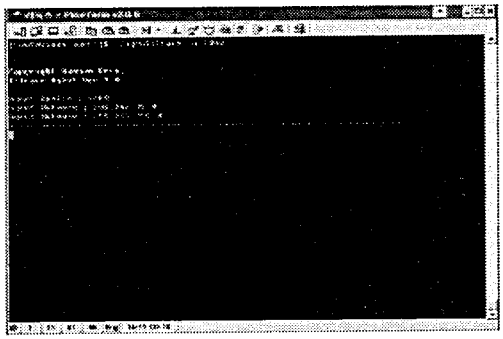

그림 4. 임계치 설정 화면

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

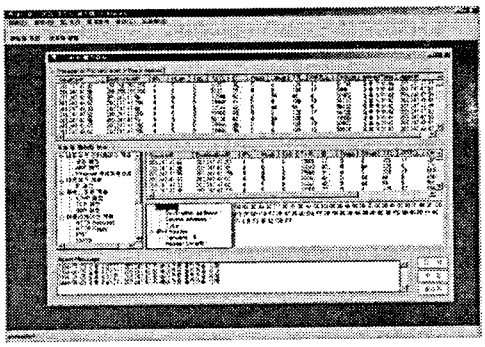

그림 5. I-Trace Manager 패킷 모니터링

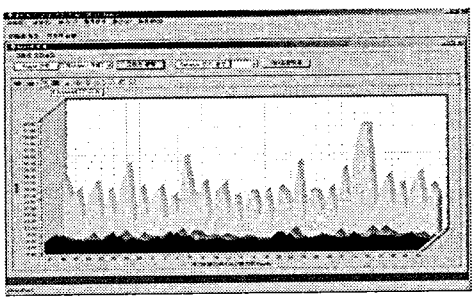

그림 6. I-Trace Manager 패킷 모니터링(그래프)

V. 결 론

인터넷 사용자의 급속한 증가로 인한 복잡한 TCP 반응과 연관되어 네트워크 서비스에 많은 패킷 손실을 야기하게 되었다. 이러한 문제를 해

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

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

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

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

[8] 이만영, 손승원, 조현숙, 정태명, 채기준 "차세대 네트워크 보안 기술" 생능출판사, pp.415-430, 2002.11.2