인터넷에서의 공격 근원지 IP 역추적 기술

이 형 우*

◈ 목 차 ◈

1. 서 론

해킹·바이러스 피해는 지속적으로 증가하고 있으며, 그 규모 역시 대형화되고 있다. 피해 정도도 급격히 확산되면서 이에 대한 적절한 대응 및 안전성 확보 기술에 대한 연구가 필요하다. 해킹·바이러스에 대한 적절한 대응능력을 갖추어야 할 것이고 적극적인 대응 방안을 설립하여 능동적인 대처가 필요하다. 국내 기업의 손실 및 피해 사례를 살펴보면, KT DNS 서버 다운 및 KIDC 서버의 다운으로 인해 국제적으로 많은 문제점을 유발하기도 하였다. 결국 이와 같은 피해가 발생하였을 때는 일차적으로 손실된 정보를 복구하는 것이 우선이겠지만, 이와 더불어 컴퓨터 범죄에 대한 추적 및 검거에 필요한 법적인 증거를 확보하고 이를 바탕으로 피해를 보상해 줄 수 있는 기술과 체계가 갖추어져야 한다. 이를 통해 기업과 국가의 경쟁력을 확보할 수 있고, 컴퓨터를 이용한 건전한 사회를 구축할 수 있을 것이다.

해킹·바이러스에 대한 대응 방안을 설정하기 위해서 백신, 침입탐지 및 침임감내 기술 등과 같은 수동적인 측면에서의 대응 방안과 공격 근원지 추적 기법과 같은 능동적인 방법으로 나눌 수 있다. 본 연구에서는 해킹 및 바이러스에 대한 능동적인 대응 방안 중에서 공격 근원지 IP를 역추적하는 기술[4,5,6,7]을 분석하고자 한다. 2장에서는 해킹·바이러스 현황 및 대응방안에 대해 살펴보고, 3장에서는 해킹·바이러스 역추적 기술을 정의하고 4장에서는 현재까지 제시된 IP 역추적 기술에 대해 살펴본다. 마지막 5장에서는 개선된 ICMP 기반 역추적 기술에 대해 고찰하며 결론을 맺는다.

2. 해킹 · 바이러스 대책

2.1 해킹 · 바이러스 현황

최근 몇 년 사이 급속도로 증가하고 있으며 특히 해킹 피해건수는 기하급수적으로 증가하고 있다. 신고되지 않은 것까지 포함한다면 가히 피해 정도는 상당한 것으로 생각된다.

초고속인터넷 최강국을 자부하는 우리나라 역시 국제 해커들의 놀이터로 전락하고 있다. 국내 최고 등급의 방화벽이 설치된 공공기관이 해킹 당하였고, 해킹방지 전문업체와 대형 인터넷 업체에도 해커가 침입했다고 발표되었다.

또한 해킹방지를 위해 설치한 방화벽과 침입탐지시스템 등 첨단 보안시스템이 해커들에게 무용지물이라는 점이다. 특히 근래에는 해킹 및 바이러스 기법이 고도화 지능화되면서 복합적으로 접목되는 추세이다. 즉 해킹 기법을 통한 취약점 분석 및 서비스 거부 공격 등의 기법과 트로이

* 한신대학교 소프트웨어학과 조교수

목마와 같은 바이러스 기법 등이 접목되어 새로운 공격 기술로 발전하고 있는 추세이다.
따라서 날로 발전하는 해킹·바이러스 기술에 대해 적절한 대처 방안 등이 제시되어야 한다. 특히 해킹 피해가 발생하였을 경우 이에 대한 방어를 위한 기술적인 보완이 필요하여 결국에는 해킹과 바이러스를 대처하고 이를 역추적하여 근원지를 검출할 수 있는 기술 개발이 필요하다.

2.2 해킹 · 바이러스 대응 방안

최근 네트워크에 대한 사이버공격 양상이 점차 복잡해지면서 단일 보안시스템만으로는 해킹·바이러스에 대한 대응이 어렵게 되었다. 또한 공격에 노출되는 네트워크 범위가 광역화되고 공격 시간도 길어지는 추세를 보이고 있다. 따라서 보안시스템 간 상호결합적 운용을 통해 글로벌 네트워크 차원에서 공격에 대한 탐지 및 대응이 가능하여야 할 것이며, 공격자에 대한 대응도 기존의 수동적 대응에서 능동적 대응 방안을 강구해야 한다.

보안 시스템은 다양한 변화에 쉽게 대처할 수 있도록 유연성과 개방성을 제공할 수 있는 '능동보안관리(Active Security Management)'기술이 필요하게 된다. 본 기술은 새로운 공격유형에 대한 강력하고도 글로벌 네트워크 차원에서의 대응방법을 강구함으로써 네트워크 보안 분야에서의 보안 신뢰도를 한차원 향상시킬 것이다.

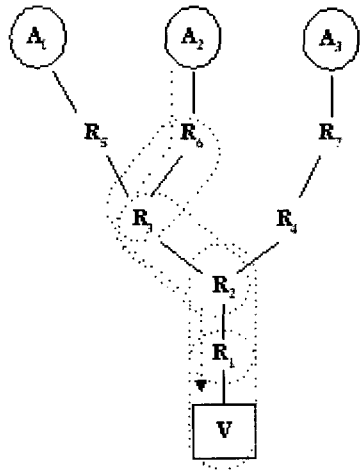
침입자의 역추적에는 DoS 공격과 같이 IP주소를 속이고서 공격하는 경우 이를 역추적하기 위한 IP 패킷 역추적 기법과 우회공격을 통해 현재 침입하고 있는 공격자의 위치를 역추적하기 위한 연결 체인 역추적 기법이 있다. 특히 IP 패킷 역추적은 분산서비스거부 공격시 IP주소를 속이는 경우가 대부분인데 실제 패킷이 전송되고 있는 위치를 확인할 수 있는 기술이다.

이러한 역추적 기법들을 활용해 실제 사용되고 있는 다양한 역추적 기술(traceback technique)들이 있는데 기본적인 로그 정보들을 활용하여 포렌식스 분석을 통한 추적기술, 역공격을 이용한 추적기술, CIS, IP추적, 커넥션 체인을 구성하기 위한 다양한 기법 등이 개발되어야 한다.

3. 해킹 · 바이러스 역추적

3.1 해킹 · 바이러스 역추적기술의 필요성

해킹사건에 사용된 수법은 분산 서비스 거부공격(DDos: Distributed Denial of service)을 할 수있는 프로그램에는 트리누가 있다. 이는 몇 개의 서버와 수많은 하부서버(클라이언트)로 이루어지는데 해커들이 트리누 마스터서버에 접속해 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부 공격을 수행하라고 명령을 내린다. 이럴 경우 트리누 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격하도록 하부서버와 통신한다. 이는 공격자의 명령에 의해 공격도구가 설치된 대량의 서버들을 제어해 공격목표 시스템에 치명적인 서비스 거부공격을 할 수 있기 때문에 전세계 인터넷을 교란시키려는 해커들에 의해 악용될 수 있다. 아래 그림 1과 같이 공격경로와 패킷의 경로는 서로 다르다는 것을 알 수 있다.



(그림 1) 패킷의 전송경로와 공격 경로

해킹·바이러스 공격이 발생하였을 경우 현재까지는 다분히 수동적인 측면에서의 대응 방안을

럽할 수밖에 없었다. 특히 기존의 방식은 해킹 시도 자체를 제한하거나 방지할 수 없는 방식으로서 결국에는 인터넷이 마비되거나 무용지물화되는 특성을 보이고 있다.

이러한 문제를 해결하기 위해서 제시된 기술이 바로 능동적인 해킹 방지 기술이다. 새로운 방식에서는 해킹 시도 자체를 방지하거나 이를 능동적으로 실시간 내에 추적할 수 있는 기술 등이 제공되어서 해킹 시도 자체를 방지하고자 하는 것이 주요 목적이다. 따라서 해킹·바이러스에 대한 능동적인 대처를 위해 필수적인 기술로 최근 그 중요도가 높아지고 있는 기술이 역추적 기술이다. 역추적 기술은 해킹·바이러스에 대한 근원지를 실시간으로 추적함으로써 해킹·바이러스에 대한 근본적인 억제 기능을 제공한다.

3.2 해킹 · 바이러스 역추적기술의 정의

역추적 기술은 능동적인 해킹 및 바이러스 대응 기법으로서 실시간으로 해커의 위치를 파악하는 것을 목적으로 하고 즉각적인 대응이 가능하도록 하는 기술을 의미한다.

기존의 수동적인 방식에서는 여러 가지 문제점이 발생한다. 실시간 추적이 불가능하고 즉각적인 대응이 불가능하여 전체 인터넷 망이 마비될 수 있는 위험성을 갖고 있다. 기존의 대응 방식은 아래 그림과 같이 해킹 시스템에서의 로그 분석을 통해 공격 시스템을 파악하고 로그 분석 과정을 반복적으로 적용하여 해킹 경로를 추적하는 수동적인 방식이었다.

로그 정보 등이 삭제된다면 전체적인 로그 분석 자체가 불가능할 것으로 판단된다. 따라서 기존의 수동적인 방법인 경우 이전 단계 추적이 어려울 경우 역추적 자체가 불가능하다는 것을 의미한다. 따라서 좀더 신속하고 정확한 실시간 역추적 시스템이 필요하다.

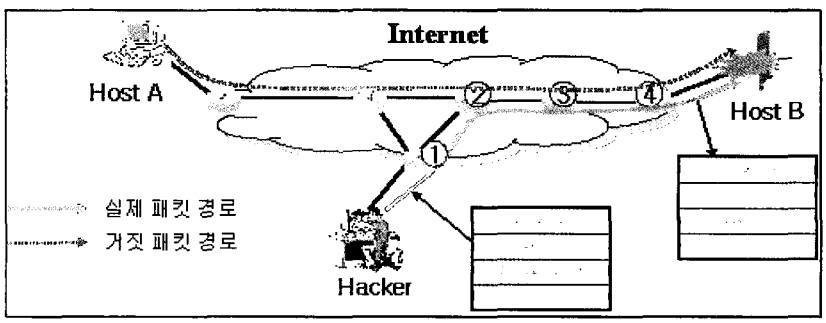
4. IP 역추적 기술

4.1 역추적 기술 분류

역추적 기술을 시스템 측면에서 분류하면 크게 IP 패킷 역추적 기술과 연결 역추적 기술로 분류할 수 있다.

- IP 패킷 역추적 기술
  (IP packet traceback technique)[5]
  · IP Address Spoofing 패킷의 실제 송신지 추적
- 연결 역추적 시스템
  (Connection traceback technique)
  · 우회 공격의 근원지 추적

IP 패킷 역추적 시스템인 경우 DoS 공격에서 IP 주소가 변경된 경우 이를 찾아내기 위한 방법을 제공한다. 아래 그림과 같이 Host B에 패킷을 보낸 시스템의 실제 위치를 추적하는 방식이다. 구체적으로 중간 경유 라우터를 이용하여 추적 경로를 유추하는 방식이다. 구체적으로 패킷에 대한 마킹 기법(Marking)을 적용한다. 즉 각 라우터에서는 패킷에 일정 확률로 선정하고 이를



(그림 2) IP 주소 변경 공격에 대한 추적

만일 추적 경로상에 있는 일부 시스템에서의 대상으로 마킹을 수행한다. 마크된 정보는 패킷

에 대한 전달 경로를 제공하게 된다.

우회 공격 근원지 추적 기법인 경우 아래 그림에서와 같이 해커는 Host B를 공격하기 위해 다수의 다른 시스템을 경유하여 해킹을 시도한다. 따라서 Host B에 존재하는 audit trail만으로는 Hacker의 실제 위치를 파악할 수 없으며, 해커의 실제 위치를 찾기 위한 여러 기법이 연구 개발되고 있다.

이와 같은 역추적 기술을 다시 세분화하면 호스트 기반 역추적, 네트워크 기반 역추적으로 구분할 수 있다.

○ 호스트 기반 역추적 시스템

호스트 기반 역추적 시스템 (Host-based traceback system) 은 모든 호스트에 역추적 모듈을 설치하는 방식이다. 따라서 모든 역추적 경로상의 호스트들로부터 정보를 얻어야 역추적이 가능한 기법이다. 기존의 모든 시스템에 역추적 모듈을 설치한다는 것이 상당히 어렵기 때문에 현재의 인터넷 환경에는 적용하기 어려운 방식이라고 할 수 있다.

○ 네트워크 기반 역추적 시스템

네트워크 기반 역추적 시스템 (Network - basedtraceback system)은 네트워크 상에 송수신되는 패킷들로부터 정보를 추출하여 존재하는 연결 정보들 간의 연관성을 파악하여 역추적 경로를 파악하는 방식이다. 예를 들어 해커가 ls 및 cd 라는 명령어를 계속적으로 입력하였을 경우 이와 같은 명령어가 흘러가는 경로를 분석하여 전체적인 해킹 및 바이러스 경로를 분석하는 방식이다. 현재의 인터넷 환경에 적용할 수 있는 가능성이 있으나, 기존의 라우터에 패킷을 감시할

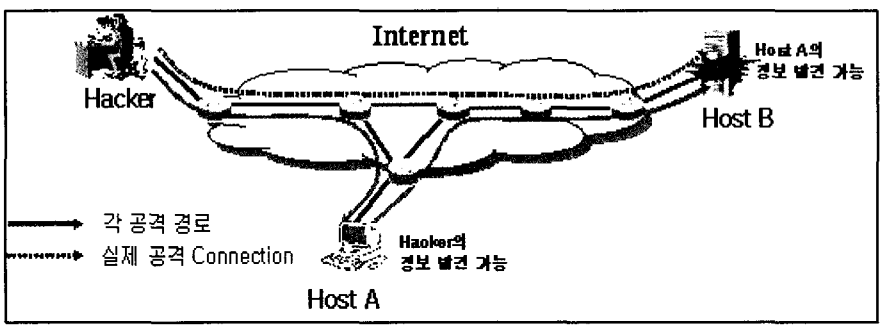
수 있는 위치에 역추적 모듈을 설치해야 하기 때문에 실제로 적용하기에는 아직도 많은 문제점을 가지고 있다.

4.2 ICMP 프로토콜

인터넷 프로토콜은 TCP/IP 프로토콜의 중심이다. IP는 OSI 참조 모델의 네트워크 계층에 해당하고, 비연결 서비스와 최선의 전달 서비스를 전송 계층에 제공한다. 특히 IP 패킷에서의 해더는 20 바이트의 고정 길이 구성 요소와 최대 40 바이트의 가변 길이의 선택적인 구성 요소를 갖는다.

헤더 구성에서 option 부분은 가변 길이로서 보안 수준, 패킷에 의하여 사용되는 경로, 각 라우터에서의 타임스템프 등과 같은 특별한 기능을패킷에 포함시키고자 하는 경우에 사용 가능하다. 또한 라우터에서 IP 패킷의 내부를 볼 수 있는 기능도 제공하고 있다.

해킹 및 바이러스가 발생한다면 서브넷을 찾고 내부 호스트 위치를 추적할 수 있는 방식이 제시되어야 한다. Van Jacobson은 'traceroute' 프로그램을 개발하여 한쪽 호스트에서 다른 호스트로 가는 IP 데이터그램의 경로를 확인하는 기능을 제공하며 IP 소스 라우트 옵션도 이용가능하다. IP header의 공간이 충분치 않기 때문에 traceroute는 IP header의 TTL field(8bit)와 ICMP[1]를 사용한다. TTL이 0또는 1이면



(그림 3) 우회 공격에 대한 추적

forward되지 못하므로 source에게 ICMP error

message(time exceeded)를 보내게 된다.

TTL 필드는 라우팅 도중에 데이터그램이 무한 루프에 들어가는 것을 방지한다. 송신자가 임의의 값을 초기화하는 8 비트 필드로서 현재는 주로 64로 설정되어 있다. Hop counter 역할을 하며 라우터에 의해 TTL 필드가 1씩 감소한다. 만일 TTL = 0 or 1이면, 다른 호스트로의 전송을 방지하며 발신지 호스트에게 ICMP time exceeded 메시지를 전송한다. 이때 ICMP 메시지에는 발신지 주소로서 router의 IP주소가 포함되어 있다.

인터넷 프로토콜은 비신뢰적이며 비연결형 전송을 제공하는 프로토콜이다. 만약 게이트웨이가 데이터그램을 전송할 수 없을 때 게이트웨이는 데이터그램을 전송한 호스트에게 어떤 형태로 에러가 발생했음을 알려줄 필요가 있다. 즉 IP의 신뢰성이 없는 면을 어느 정도 보완하기 위하여 게이트웨이와 호스트간의 에러 정보 교환을 가능하게 하는 프로토콜이 요구되는데 이를 위하여 고안된 것이 바로 ICMP이다.

ICMP 메시지 형식은 일단 헤더와 데이터영역으로 나뉘어지는데 헤더는 ICMP의 메시지 타입에 따라 약간씩 다르기는 하지만 최소한 메시지 타입에 대한 정보와 그것을 좀더 상세히 알려주는 코드를 가지고 있다. 그리고 데이터 영역에는 문제가 있는 데이터그램의 헤더와 처음 64bit의 내용이 들어가 있다. 이 안에는 특정 연결에만 ICMP의 메시지가 전달될 수 있도록 참조할 수 있는 내용이 들어있으며 상위 레벨의 프로토콜에서 발생한 에러에 특정 행위를 할 수 있는 정보를 내포한다.

4.3 ICMP 기반 역추적 기술에 대한 고찰

ICMP에서 발생할 수 있는 보안 문제는 크게 두 가지로 나눌 수 있다. 첫째는unreachable type 표기 문제이고 두 번째는 redirect 공격이다.

unreachable type은 원하는 호스트(또는 게이트웨이)로 데이터가 전송될 수 없음을 알려주는 메시지이다. 그런데 실제로 reachable한 호스트를 unreachable하다고 하는 경우 문제가 발생할 수 있다.

예를 들면 isis라는 호스트가 horus는 unreachable 하다는 ICMP 메시지를 받으면 isis에서 horus로 가는 모든 데이터는 버려지게 된다(즉 연결이 끊어지게 된다). 비록 horus가 실제로는 살아 있더라도 isis는 받은 ICMP를 그래로 믿어 horus를 unreachable한 호스트로 여기는 것이다.Unreachable ICMP 메시지를 보내는 것은 간단한 프로그램을 통하여 쉽게 구현할 수 있다.

또한 redirect를 이용한 침입은 보안에 지대한 영향을 미칠 수 있다. 위에서 언급한 것처럼 redirect 메시지는 게이트웨이가 라우팅 경로를 바꾸도록 호스트에게 전달하는 메시지이다.
어떠한 네트워크나, 노드 상에서 에러가 발생될 경우 이를 각 송신지 호스트에 통지할 수 있는 기능이 필요하게 되고, 이러한 목적에 의해 ICMP가 사용된다. 모든 IP 구현의 공통 요소이며, IP를 위한 에러 및 진단 데이터를 전송한다. ICMP는 다양한 정보를 전송할 수 있고 ICMP의 프로토콜 헤더의 기본 부분만 고정된 구조를 가지며 각 필드의 의미는 경우에 따라 가변적이다. 따라서 ICMP 구조에 추적 정보를 포함시켜 이를 이용하여 역추적에 이용할 수 있을 것으로 판단된다.

코드는 지정된 타입 내에서의 세부 기능을 나타내고, Checksum은 전체 ICMP를 위한 Checksum field이며, 기타 부분은 기타 목적(일련번호, 인터네트 주소 등)을 위한 정보를 표시한다. 또한 IP 프로토콜 헤더에는 문제가 발생한 IP 데이터그램과 메시지의 8바이트에 해당하는 앞 부분이 담겨 있다. 문제가 TCP나 UDP 메시지에서 시작되었다면 대응 TCP나 UDP 프로토콜 헤더 부분과 에러 메시지의 8바이트에 해당하는 앞부분이 담겨지게 된다. 에코의 요청이 있을 경우에는 테스트 데이터가 담겨질 수도 있다. ICMP 메시지는 IP, TCP 및 UDP에 의해서만 발생되며, 이미 발생한 ICMP 메세지에 대한 응답으로 또다른 ICMP 메시지가 발생될 수 없다.

결국 IP 패킷의 내부에 역추적 경로 등을 마킹하고, ICMP 프로토콜을 사용하여 역추적에 적용하여 해킹 및 바이러스에 실시간으로 대응하는 기술에 해당한다. 또한 근래에는 워터마크기

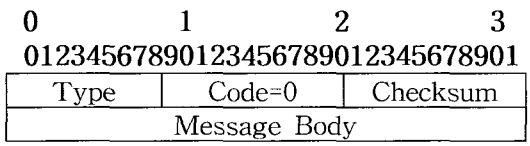
술의 개념을 패킷 마킹 기술 등에 적용하여 역추적 정보를 은닉하는 기술에 대해 연구되고 있다. 이와 같은 마킹 기법은 확률론적 방법을 사용하여 패킷을 샘플링하고 여기에 특정한 IP 주소 정보를 은닉하는 기법이다.

5. ICMP 기반 역추적 기술

인터넷을 통해 패킷이 전송되는 경로를 추적하는 기술이 제시되어야 한다. 특히 DoS 공격에 대처하기 위해서는 근원지 IP이 위조 및 변경되기 때문에 패킷 경로에 대한 동적 역추적 기술이 필요하다. 물론 traceroute와 같은 툴이 제공되고 있으나 이는 전방 경로 추적을 제공할 뿐 역경로 추적 기술은 제공하지 못하고 있다. 따라서 이와 같은 문제를 해결하기 위해 개선된 ICMP 기반의 역추적 방식[7]이 제안되었다. 패킷을 전송할 때, 라우터는 확률적으로 역추적 메시지를 목적지를 따라 전송하거나 근원지로 전송하게 된다. 따라서 어느정도 충분한 양의 역추적 메시지가 있다면 패킷의 근원지와 경로를 추적할 수 있다.

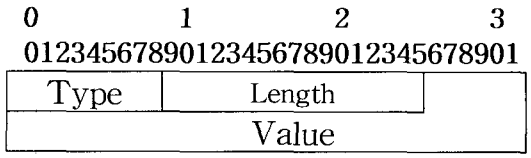
5.1ICMP역추적메시지

IPv6에서의 ICMP 역추적 메시지 구조는 아래와 같다. ICMP 메시지는 type 부분과 code 부분 및 checksum 부분으로 구성되며, 다음에 메시지 내용으로 구성된다.



(그림 4) 역추적 메시지 구조

메시지 내용 부분은 다시 아래와 같은 형태로 구성된다. 즉, ICMP 역추적 메시지는 TLV (type-length-value)의 재귀적인 구조로 구성된다. 즉, 그림 4와같은 ICMP 메시지에서 내용 부분에 해당하는 사항은 다음 그림 5와 같은 구조로 생성되며, 그림 5의 메시지 구성은 재귀적인 형태로 구성되는 방식이다.



(그림 5) 역추적 메시지 본문의 세부구조

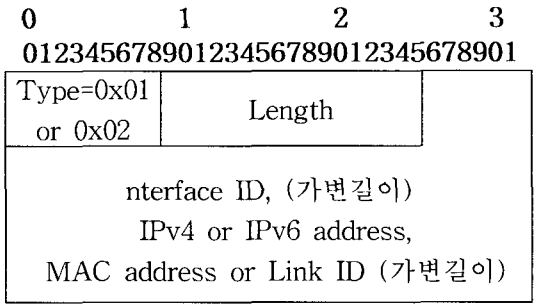
Type 부분은 0x01부터 0x7f까지가 상위값에 해당하고 0x81부터 0xff까지는 메시시 내용에서의 type 값에 해당하는 옥텟 정보로 구성된다. 상위 및 하위 레벨에서의 type 값은 아래와 같다.

Type	Element Name (상위 메시지)
0x01	Back Link
0x02	Forward Link
0x03	Timestamp
0x04	Traced Packet Contents
0x05	Probability
0x06	RouterId
0x07	HMAC Authentication Data
0x08	Key Disclosure List
Type	**Element Name (하위 메시지)**
0x81	Interface Name
0x82	IPv4 Address Pair
0x83	IPv6 Address Pair
0x84	MAC Address Pair
0x85	Operator-Defined Link Identifier
0x86	Key Disclosure
0x87	Disclosure Signature

(그림 6) ICMP 메시지 형태 분류표

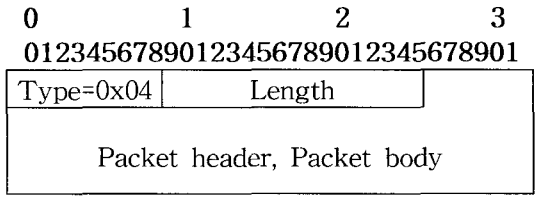
ICMP 역추적 메시지는 전방 및 후방 링크 정보를 포함하고 있어야 한다. 즉 목적지까지의 링크 정보 혹은 근원지까지의 링크 정보를 포함하고 있어 경로에 대한 체인을 구축하게 된다.

value 필드 값에는 근원지 및 목적지의 IP 주소값 등을 포함하게 된다. 구체적으로 back link(type=0x01) 및 forward link(type=0x02)에 해당하는 경우 아래와 같은 구조로 ICMP 메시지가 구성된다.



(그림 7) back/forward link 메시지 구조

timestamp(type=0x03)인 경우 FRC1305에 기반한 구조를 사용하며 traced packet(type=0x04)인 경우 역추적 패킷의 내용을 포함하게 되며 아래와 같은 구조이다.

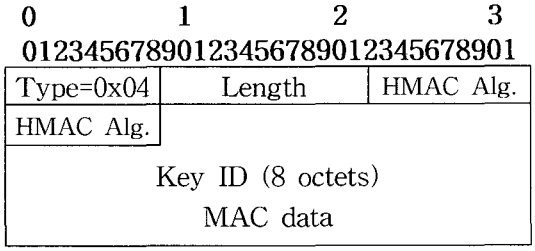


(그림 8) traced packet 구조

5.2 ICMP 역추적 메시지 인증

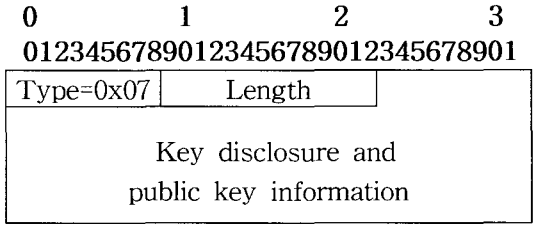
이와 같은 패킷에 대해 공격자 역시공격 근원지를 감추거나 다양한 형태의 공격을 수행하기 위해 역추적 메시지를 생성할 수 있기 때문에 ICMP 역추적 메시지에 대한 인증 과정을 수행해야 한다.

이를 위해 사용할 수 있는 대표적인 방식이 디지털 서명을 이용하는 것이지만 라우터에서 이와 같은 과정을 수행하기에는 무리가 따르기 때문에 대신에 해쉬 방식을 적용한 HMAC[2] 인증 방식(type=0x07)을 사용한다. 공개키 방식에 기반하고 키 공유 방식을 사용하며 아래와 같은 구조로 생성된다.



(그림 9) HMAC 인증 메시지 구조

또한 키공개리스트 (key disclosure list : type = 0x08)를 통해 HMAC 인증 메시지를 생성하는데 사용된 키 목록을 포함하게 된다. 물론 key disclosure 서브 메시지(type=0x86)인 경우 이전 ICMP 역추적 메시지의 인증에 사용하기 위한 키를 포함하고 있다.



(그림 10) key disclosure list 구조

ICMP 역추적 기능을 제공하는 라우터에서는 ICMP 역추적 메시지를 대략 1/20,000의 확률로 생성하고 랜덤하게 선택된 패킷의 근원지 또는 목적지에 ICMP 패킷을 전송하게 된다. ICMP 패킷 생성률은 대략적으로 1/20,000로 설정하며 평균적으로 20홉을 거친다고 할 때 0.1%의 트래픽 증가를 가져온다. 패킷 선택 과정은 의사난수 방식을 사용하게 된다.

즉, 개선된 ICMP 기반 역추적 기법에서는 후방 경로에 대한 링크 정보를 제공하기 위한 ICMP 역추적 정보를 생성하거나, 전방 경로에 대한 ICMP 메시지를 생성하여 근원지 또는 목적지로 전달하고 메시지에 대한 인증을 위해 HMAC 방식을 사용하여 ICMP 역추적 경로 정보의 변형을 방지하게 된다. 물론 이를 위해서는 공개키 기반의 키정보를 활용하며 키공개 목록

및 키공개 과정에서는 디지털 서명 기법이 적용되고 있다.

5.3 향후 역추적 기술 동향

앞에서 제시한 ICMP 기반 역추적 기술을 비롯하여 확률적으로 선택된 패킷에 대한 마킹 과정을 통한 기법, 네트워크 기반의 역추적 기술과 해쉬 방식을 통한 역추적 기술 등이 제시되고 있다. 기술 발전과정을 살펴보았을 때 초기에 제시된 마킹 기반의 역추적 기술은 구현과정에서 문제점을 가지고 있으며, 따라서 가장 효율적인 방식으로는 해쉬 방식에 기반한 단일 패킷 역추적 방식이 제시되고 있다. 네트워크적인 측면에서는 라우터를 통한 ICMP 패킷을 생성하는 방식이 제시되고 있으며 역시 HMAC을 이용한 역추적 경로 추적 방식이므로 이와 같은 두가지 방식을 결합한 방식이 역추적 기술에서는 바람직하며 또한 액티브 네트워크 또는 지능형 네트워크를 구성하는 라우터가 구축된다면 역추적 경로를 제공할 수 있는 스마트 패킷에 대한 연구도 진행되고 있다.

6. 결 론

본 연구에서는 인터넷을 통해 급격히 확산되고 있는 해킹·바이러스에 대한 대응 기술로서 DoS 공격 등을 수행하는 과정에서 근원지 IP를 역추적하는 기술에 대해 살펴보았다. 역추적 기술의 필요성과 현황 및 대응 방안을 중심으로 기술하였으며, 현재까지 제시된 IP 역추적 기술을 제시하고 특히 라우터를 중심으로 패킷에 대해 전방 경로 또는 후방 경로에 대한 정보를 ICMP 패킷으로 생성하여 전달하는 방식에 대해 고찰하였다.

참 고 문 헌

[1] J. Postel, "Internet Control Message Protocol", RFC 792, Internet Engineering Task Force, September 1981.

[2] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, Internet Engineering Task Force, February 1997.

[3] Deering, S. and R. Hinden, "Internet Protocol, Version 6, (IPv6) Specification", RFC 2460, December 1998.

[4] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[5] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback", Technical Report UW-CSE-2000-02-01, Department of Computer Science and Engineering, University of Washington

[6] A.C. Snoeren, C. Partridge, L.A. Sanchez, W.T. Strayer, C.E. Jones, F. Tchakountio, and S.T. Kent, "Hash-Based IP Traceback", BBN Technical Memorandum No. 1284, February 7, 2001.

[7] Steve Bellovin, Tom Taylor, "ICMP Traceback Messages",RFC 2026, Internet Engineering Task Force, February 2003.

◐ 저 자 소 개 ◑

이 형 우

1994년 고려대학교 전산과학과 (이학사)
1996년 고려대학교 전산과학과 (이학석사)
1999년 고려대학교 전산과학과 (이학박사)
1999년~2003년 천안대학교 정보통신학부 조교수
2003년~현재 : 한신대학교 소프트웨어학과 조교수
관심분야 : 정보보호, 네트워크보안, 컨텐츠보호기술, 정보은닉 등