IP 역추적 기술에 대한 기술적 및 환경적 한계에 관한 연구

황성철[0] 우연옥 강흥식
인제대학교 전산학과
{mslove1[0], poppi99}@nate.com

hskang@cs.inje.ac.kr

A Study on Limit of technique and environment about IP traceback Technology

SungChul Hwang[0] YeaonOk Woo HeungSeek Kang
Dept. of Information and Computer Engineering, Inje University

요 약

IP 역추적 기술이란 침입을 시도하는 공격자의 위치를 실시간으로 추적하는 기술을 말한다. 이러한 역추적 기술은 현재까지의 어떠한 보안강화 방법이나 도구들 보다 능동적인 성격을 갖고 있으며, 오늘날에도 많은 연구가 활발히 진행되고 있는 분야이다. 하지만 지금의 역추적 기술들을 인터넷이라는 환경에 바로 적용하기에 많은 문제점들을 가지고 있다. 역추적 기술이 완벽히 수행되지 못하는 이유는 현재 인터넷 환경이 가지고 있는 수많은 가변적 요인들 때문이다. 그러므로 역추적 방법을 실현하기 위해서는 지금현재 사용중인 인터넷 환경에서 곧바로 적용할 수 있는 방법들에 대한 연구가 필요하다. 본 논문에서는 최근 2~3 년 사이에 발표되었던 역추적 기술에 대한 소개와, 해당하는 기술들의 문제점을 지적함으로서 앞으로의 역추적 기술에 대한 실질적인 정보를 제공하고자 한다. 또한 역추적 기술의 적용에 가장 큰 문제점으로 작용하는 인터넷 환경의 문제점들을 파악하고자 한다.

1. 서 론

해마다 일어나는 사이버 범죄에 대한 방어기술들은 지능형IDS, 자동 보안패치를 비롯해 많은 발전을 보이고 있다. 하지만 이에 대한 사이버 범죄의 공격유형이 보안기술들에 비해 더욱 빠른 기술적 형태를 갖추고 있기 때문에 현재까지 인터넷에서 일어나는 많은 범죄행위에 대해서 대부분의 시스템들이 완벽한 보안을 이루어내지 못하고 있는 것이 사실이다. 또한 이러한 보안강화 도구들은 사후 처리에 핵심을 두고 있기 때문에 공격자의 범죄행위들에 대한 근본적인 보안의 개념은 현재까지 많이 미비한 실정이다. IP 역추적 기술이 실제 인터넷 환경에 적용하기에 많은 문제점이 있지만, 현재까지 계속해서 연구되고 있는 이유 중 하나가 바로 사전대응 이라는 성격 때문이다. 공격자의 심리적인 불안감을 증폭시켜 공격시도 자체를 줄일 수 있다는 것은 앞으로의 사이버 범죄에 예방차원에서도 반드시 이루어야할 과제인 것이다. 이러한 IP 역추적 기술들은 80년대부터 오늘날까지 계속해서 연구되어온 기술이지만 아직은 실제 인터넷 환경에 적응하기에는 많은 문제점들이 따른다.

본 논문에서는 이러한 IP 역추적 기술 중 가장 최신의 기술들에 대해서 살펴보고, 최신 기술들이 가지는 문제점을 파악할 것이다. 더불어 현재 인터넷 환경에서 왜 이렇게 IP 역추적 기술의 적용이 어려운지에 대해서도 살펴볼 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 최근 가장 활발히 연구되고 있는 몇 가지 IP 역추적 기술에 대해서 알아보며, 3장에서는 IP 역추적 기술이 인터넷 망에 적용하기 어려운 이유에 대해서 언급하며 끝으로 4장에서는 본 논문의 결론 및 IP 역추적 기술에 대한 향후 과제에 대해서 언급한다.

2. 관련 연구

2.1 패킷 마킹 기법

패킷 마킹 기법[1]은 네트워크에서 전송되는 패킷에 대해 라우터가 고정된 확률을 통해서 패킷에 마킹하는 방법을 말한다. 즉, 라우터에서 전송되는 패킷에 대한 경로정보를 마킹한 후, 다음 라우터에서 재확인, 마킹 등의 순서를 거쳐서 이루어지는 기술을 말한다. 이런 식으로 마킹된 패킷을 받은 피해 호스트는 마킹된 패킷을 이용하여 공격자의 근원지를 네트워크에서 찾아가는 방법을 사용한다. 패킷 마킹 기법에 사용되는 방법은 크게 4가지로 이루어져 있으며, 4가지의 기법은 모두 동일한 기본 개념을 가지고 있다. 패킷 마킹 기법의 기본 개념은 공격자로부터 피해호스트까지 전송되는 패킷 중 확률을 만족하는 패킷을 라우터가 마킹하는 것을 기본으로 출발한다. 마킹된 패킷의 수가 충분히 도착했을 경우, 피해호스트로부터 공격자까지의 위치는 해당되는 라우터로부터 마킹된 패킷의 정보를 보고 알 수 있게된다.

2.1.1 패킷 마킹 기법의 한계점

패킷 마킹 기법은 실제 사용되고 있는 인터넷 환경에 적용할 수 있는 가장 손쉬운 방법 중 하나이다. 하지만 이 기법은 취약점은 네트워크에서 전송되는 패킷의 노드가 변경된다면 아무런 정보도 얻을 수 없다는 것이다. 그렇기 때문에 현재의 인터넷 망에서 사용중인 가변적

경로의 라우팅 방법에 대해서는 역추적의 효과가 거의 없다는 문제점을 안고 있다.

2.2 SWT(Sleepy Watermark Tracing)

SWT[2][3] 기법은 패킷 워터 마킹[4]이라는 방법을 사용하는 대표적인 역추적 기법이다. SWT의 기본적인 동작구조는 침입에 대한 응답 패킷에 워터마크라는 특정 정보를 삽입하여 역추적을 수행하는 원리를 가진다. SWT의 특징은 공격에 대한 응답 패킷을 이용하여 공격자의 위치를 추적하기 때문에 정확하고 신속한 역추적이 가능하다는 것이다.

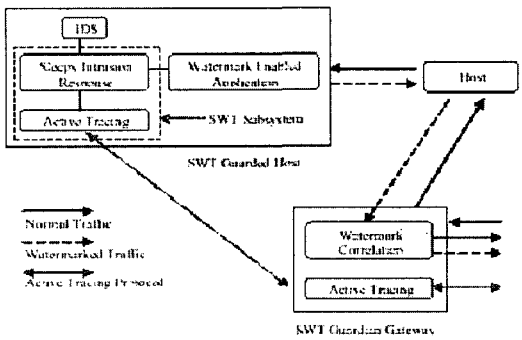

그림1. SWT 구조

그림1에서 하나의 네트워크에 보조 게이트웨이(Guardian Gateway)rk 존재하고, 이것과 동시에 연동해서 동작하는 Guarded Host가 존재한다. 공격자의 최초 침입 시도시점에서는 아무런 추가적인 동작이 진행되지 않는 일반적인 상태로 존재하게 되지만, 침입이 발생하게 되면 Guarded Host내에 존재하는 IDS가 이를 탐지하게 된다. 또한 이와 동시에 Guarded Host의 SWT subsystem에서 sleepy intrusion response 모듈이 작동을 시작하고 이때부터 일반 host에 도착되는 패킷에 의한 응답이 Watermark Enable Application에 의해 이루어지게 된다. 그렇게 되면 어플리케이션은 일반적인 응답패킷에 워터마크를 삽입하여 전송하기 시작한다. 또한 역추적이 시작되면 어플리케이션은 보조 게이트웨이(Guardian Gateway)의 Active Tracing모듈과 연동되어 워터마크가 삽입된 패킷을 찾기 시작한다.

SWT기법은 현재까지의 역추적 기법 중 가장 빠르고 정확한 역추적 결과를 얻을 수 있는 연구라고 할 수 있다.

2.2.1 SWT기법의 한계점

SWT기법 역시 현재의 인터넷에 적용하기에는 많은 문제점을 가지고 있다. 먼저 인터넷에 연결되어 있는 모든 호스트에 Watermark Enable Application이 설치되어져야만 하며, 이것은 실제로 거의 불가능에 가까운 가정이라고 할 수 있다. 설령 위의 말대로 모든 호스트에 Wateramark Enable Application이 설치가 되어서 동작을 하더라도 네트워크 부하에 따른 속도저하, 비용증가 등의 많은 문제점을 가지게 된다. 또한 공격자가 사용하는 패킷이 암호화 되어진 패킷 전송이라면 SWT기법으로는 더 이상 역추적을 수행할 수 없게 된다.

2.3 IPv6 역추적 기법

현재의 인터넷 프로토콜인 IPv4를 이용한 인터넷 환경에서 IPv6로 프로토콜이 변경된다면 네트워크의 많은 부분이 수정, 변경, 보완 되어야 할 필요가 있다. 이에 맞춰 새로운 형태의 역추적 기법에 대한 제안이 국내외에서 활발히 연구되고 있는 실정이다.

2.3.1 IPv6 헤더

IPv6에 관련된 역추적 기법들을 소개하기 전에 IPv6의 헤더에 대해서 이해해야 할 필요가 있다.

Version	Traffic Class	Flow Label	
Payload Length		Next header	Hop Limit
Source Address			
Destination Address			

표 1 IPv6 기본 헤더

표1에서는 IPv6 프로토콜의 기본 헤더 구성을 보여주고 있다. 위의 표에서와 같이 IPv6의 헤더에는 모두 8개의 구성요소로 이루어져 있으며, 기본적으로 64비트의 고정된 값이 이루고 있다. 따라서 IPv6는 기본적으로 64비트 처리가 가능하도록 만들어져 있다.

Payload Length는 현재의 헤더 뒤에 따라오는 모든 Payload의 바이트 수를 말하며, Next Header는 수신측 컴퓨터 주소 필드 뒤에 따라오는 옵션 헤더의 타입을 결정하며, Hop Limit는 라우터를 하나 거칠 때 마다 1씩 줄어드는 값이다. 트래픽 분류의 값은 Upper Layer에서 읽을 수 있다는 점에서 TCP/UDP의 어플리케이션에서 요구하는 QoS를 지원하기 위해 IP Layer가 하단의 전송 계층에게 이를 요구하는 경우를 위한 배려이다. Flow Label은 트래픽 분류를 받아서 이를 송신측 컴퓨터에서 수신측 컴퓨터까지의 모든 라우터에서 만족하기 위해 지정하는 것이다. 이것은 RSVP(Reservation Protocol)과 같은 자원예약 프로토콜의 사용이 요구되며, 라우터에서 확인 절차를 거쳐 자원예약이 성립되어야 하는 과정을 거치야 한다.

2.3.1 역추적 기법 제안

IPv6에서 제안[4]하고 있는 역추적 기법은 트래픽 클래스와 플로우 라벨을 이용하는 방법이다. 이들은 모두 QoS를 보장하기 위해 사용되어지는 필드들이다. 이 필드는 사용자가 디폴트가 아닌 서비스 품질 혹은 실시간 서비스와 같은 특별한 처리를 요구하는 트래픽 흐름에 속하는 패킷을 레이블링 할 수 있다. 이러한 특징을 이용하여 패킷 워터마크 기법을 적요해서 각각의 필드에 특정 Signature를 워터마크를 이용해 삽입한다.

IPv6의 플로우 라벨 필드에 역추적 메시지를 마킹하며, 트래픽 클래스 필드에는 현재의 홉의 라우터의 주소와

이전 홉의 라우터의 주소를 마킹하게 된다. 즉 공격 경로를 저장하고 있으므로 저장된 공격 정보를 공격정보 경로를 가지고 역추적을 수행할 수 있게 된다. 또한 IP 스푸핑 방법을 통한 공격의 경우에도 IPv4의 IP 주소와 MAC 주소를 조합하여 생성한 IPv6 주소를 플로우 라벨 필드에 암호화 알고리즘을 이용해서 마킹하는 방법을 통해 역추적이 가능할 수 있게 할 수 있다.

3. 역추적 기술의 적용에 관한 문제점들

3.1 IP Spoofing

공격자의 공격 유형 중 가장 흔하게 사용하고 있는 방법이다. 이 방법은 실제 공격자의 IP를 다른 IP로 속여서 목적호스트를 공격하는 방법으로, 공격자의 위치를 알아냈다고 하더라고 이것은 실제 공격자의 위치가 아닌 다른 IP 주소를 나타내게 된다.

3.2 인터넷 환경의 가변성

인터넷 환경은 NAT, 터널링, 가상IP, 동적IP 등과 같은 다양하고 복잡한 구조로 이루어져 있다. 이것을 하나의 알고리즘이나 기법을 이용해서 실제 공격자의 위치를 역추적 하기에는 환경상의 많은 문제점을 만들어 내는 요인이 된다.

3.3 우회 기법을 이용한 공격

실제 공격자의 위치를 속이는 방법과는 달리 목적호스트를 공격하기 위해 하나 이상의 다른 호스트들을 거쳐서 목적 호스트를 공격하는 방법을 말한다. 이 방법으로 공격을 당한 피해호스트에서 공격자의 실제 위치를 알기 위해서는 시간적, 위치적, 인력 등과 같은 많은 문제점을 야기시키게 된다.

3.4 유일성 조건에 대한 값의 부재

현재의 인터넷 환경에서는 공격자의 위치를 알아내기 위한 유일한 조건값이 없는 상태이다. 만일 IPv6로 프로토콜이 변경된다면 다시 생각해 봐야 할 문제이지만, IPv4 프로토콜을 사용하는 현재로서는 이러한 유일성 값은 존재하지 않고 있다.

3.5 역추적 수행시간의 문제

원래 역추적 기술은 실시간으로 공격자의 위치를 파악하는 것이 중요한 목적이 된다. 하지만 현재의 기법들을 인터넷 망에 적용했을 경우 역추적을 수행해서 결과를 얻는 시간이 너무 많이 소요된다는 것이다. 공격자들의 공격시간을 고려했을 때 역추적 기법들의 수행 시간은 공격자들이 범죄행위를 행한 후 에도 더 많은 시간을 소요하게 된다.

3. 6 라우팅 환경의 문제

현재 인터넷 환경에서 사용하고 있는 라우팅 기법은 크게 두 가지 경우로 나누어 질 수 있다. 첫 번째는 거리 벡터를 이용한 방법이며, 두 번째는 링크 상태를 이용한 기법이 그것이다. 문제는 라우팅 기법의 특성상 패킷 전송에 사용되는 네트워크 노드들은 고정적인 패스를 사용하지 않고 가변적인 라우팅을 사용한다는 것이다. 즉 노드의 상태 혹은 라우터의 하드웨어적인 문제 등에 의해 패킷전송에 사용되는 네트워크의 노드들은 수시로 변할 수 있다는 것이다. 현재까지의 역추적 기법들은 이렇게 수시로 변할 수 있는 네트워크 노드에 대한 정보를 실시간으로 처리해서 공격자를 역추적 하기에는 보다 많은 연구를 필요로 한다.

3.7 프로토콜의 저장공간 부족

현재 사용중인 IP(Internat Protocol)의 헤더에는 고정되어있는 크기의 헤더가 존재한다. 하지만 이러한 헤더의 크기에 역추적에 관한 정보를 저장하기에는 비어있는 헤더의 용량에 문제가 따른다. 즉, 지금 사용하고 있는 IP헤더의 저장공간에는 역추적 정보를 저장하기 위한 공간이 부족하다는 것이다. 이 문제는 IPv6로 버전 업 되는 과정에서는 반드시 바뀌어야 할 문제들이다.

4. 결 론

역추적 기술에 대한 적용은 지금 사용중인 인터넷 환경에서는 아직 많은 문제점들을 가지고 있다. 그 이유는 현재의 인터넷 환경이 너무 복잡하고, 가변적인 요소들을 많이 가지고 있다는 것이다. 단, 이것은 인터넷이라는 네트워크 형태에 대한 환경상의 문제점이라는 것이다. 보다 현실적이고 실제 적용가능한 역추적 기법을 위해서는 이러한 가변적 요소에 대한 기술적 부분이 좀 더 보완되어야 할 것이다. 또한 역추적 기술의 특성상 지금 사용중인 어떠한 보안 강화 도구들 보다 사이버 범죄 예방에 대한 뛰어난 대비책이 될 수 있으므로 앞으로도 많은 연구를 필요로 하고 있다.

참고문헌

[1] http://www.cisco.com
http://ccl.cun.ac.kr
패킷 마킹을 위한 IP 역추적 기술 -한국전자통신연구원

[2] Xinyuan Wang, Survivability Through Active Intrusion response

[3] Xinyuan Wang, Sleepy Watermark Tracing : An Active Network Based Intrusion Response Framework

[4] IPv6의 공격근원지 역추적 모델 연구 - 전북대학교 컴퓨터공학과
http://www.ipv6.or.kr
http://www.ipv6.org
http://www.i2r.a-star.edu.sg
http://www.ietf.org/proceedings/01mar/slides