사이버공격 근원지 역추적 기술

한국전자통신연구원(ETRI)부설연구소

1. 서 론

분산서비스거부공격(DDoS ; Distributed Denial of Service), 스캐닝 공격 등은 지속적으로 발생중인 사이버위협으로 이러한 공격에 대응하기 위해서는 공격자의 위치 및 호스트를 파악하여 필터링하고 제거하는 것이 효과적이다. 하지만 공격자 호스트들은 자신들의 위치를 은폐하기 위해 소스 IP 주소를 위장(Spoofing)하므로 공격 경로를 역추적하는데 어려움이 있다. 역추적 기술은 공격자 호스트를 찾아 필터링을 수행하거나 제거하는 기술로 사이버공격에 가장 효과적인 대응 중에 하나이다. 사이버공격 근원지 역추적 기술은 2003년도까지 많은 연구자들이 연구를 수행하였으며, IETF에서 표준을 지정하고자 하는 시도도 있었다. 하지만 현재까지의 연구 결과들은 연구 수준에 그치고 있으며 실제 적용된 사례는 찾아보기 힘든 상황이다. 이에 본 문서에서는 한신대 이형우 교수가 정보보호학회 논문지에 2003년도 12월 게재한 논문과 올해 12월 LNCS에 발간될 ETRI 서정택 박사의 논문 그리고 CIAS-ISSA Security Symposium 2007에서 발표된 Southwest Research Institute의 PPT 자료를 기반으로 하여 그동안의 역추적 관련 연구내용을 분석하고, 향후 역추적 기술의 연구 및 실용화 방안에 대하여 논의하고자 한다.

2. 2003년 말까지의 공격근원지 역추적 기술 동향

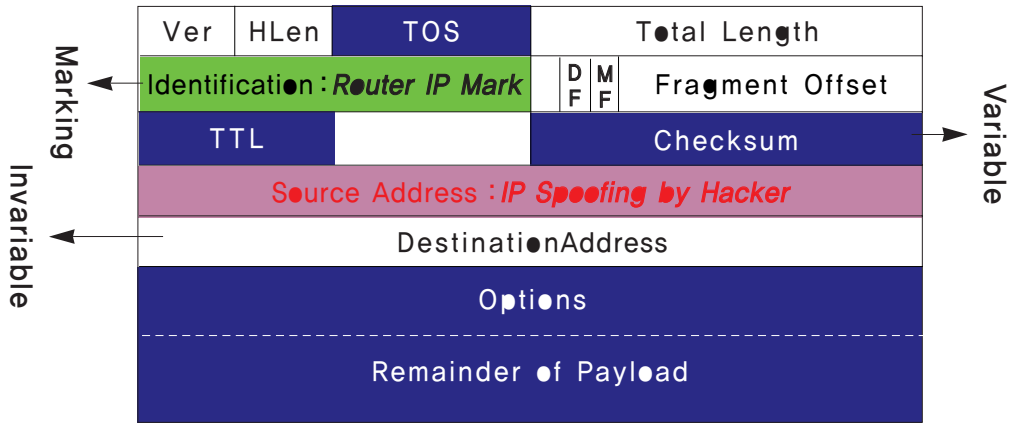
2003년 말까지의 연구결과들을 보면 인터넷에서의 패킷 특성상 TCP 계층을 중심으로 한 서비스 중심의 역추적 기능 보다는 패킷 자체의 네트워크 전송 과정을 다루는 IP 계층에서의 역추적 기능을 제공하기 위한 연구가 활발히 진행되었다. 따라서, IP 계층을 중심으로 현재까지 제시된 역추적 기술을 분류하면 해킹 대응 방식에 따라 크게 전향적(Proactive) 역추적 기술과 대응적(Reactive) 역추적 기술로 나눌 수 있으며, 세부 기술로 나누어 본다면 라우터 중심의 역추적 기술, 패킷 정보에 대한 관리 시스템 구현 기술, 특수 네트워크 중심 기술 및 관리 기술 중심의 역추적 기술로 분류할 수 있다.

가. 전향적 역추적 기술

본 기술은 네트워크상에 패킷이 전송되는 과정에서 사전에 역추적 경로 정보를 생성하여 패킷에 삽입하거나 목적지로 전달하여 주기적으로 관리하면서 만일 해킹 공격이 발생하면 이미 생성, 수집된 정보를 이용하여 해킹 공격 근원지를 판별하는 기술이다. 구체적으로 분류하는 패킷에 대한 확률적 마킹(PPM : Probability Packet Marking) 기법과 전통적인 ICMP 메시지를 변형한 iTrace(ICMP Traceback) 기법으로 나눌 수 있다.

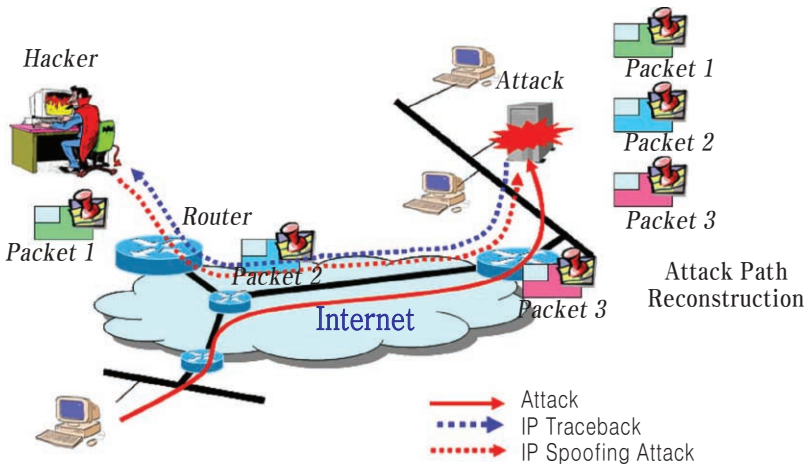
(1) PPM 역추적 기법

위장된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크상에 전송되는 패킷에 대해 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다. 즉, 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더의 변형 가능한 필드에 해당 라우터의 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다. **[그림 1]**과 같이 IP 헤더의 16비트 ID 필드에 라우터 자신의 IP 주소정보를 삽입할 수 있다.



[그림 1] IP 헤더 형태

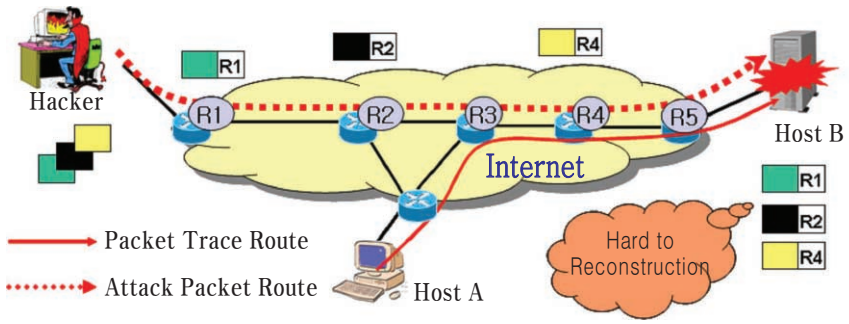
각 라우터에서 삽입된 정보는 다시 다음 라우터로 전달되고 최종적으로 목적지 공격대상 시스템에 전달된다. [그림 2]와 같이 각 라우터에서 마킹된 정보가 전달되면 추후에 해킹 공격이 발생하였을 경우, 해킹 공격에 해당하는 패킷에 기록된 라우터 정보를 재구성(reconstruction)하여 실제적인 패킷의 전달 경로를 재구성한다.



[그림 2] PPM 기법 구조

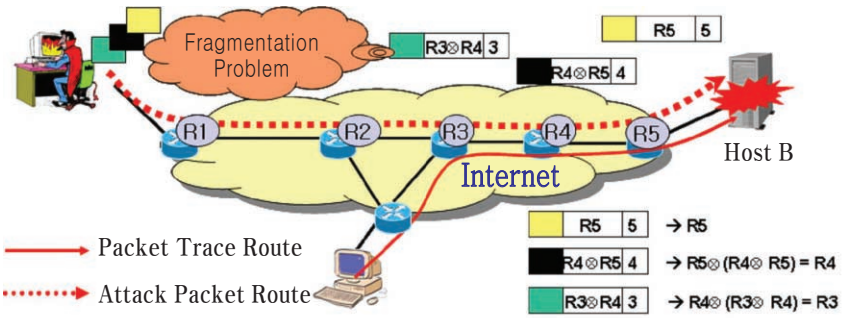
각 라우터에서 전달된 정보를 마킹하는 과정에서 모든 패킷에 마킹하게 되면 전체 네트워크의 지연 현상이 발생하기 때문에 일반적으로 라우터에서는 확률 p로 패

킷을 샘플링하여 마킹하게 된다. 이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링(Node Sampling), 에지 샘플링(Edge Sampling) 및 개선된 패킷 마킹 기법 등이 제시되었다. [그림 3]과 같이 노드 샘플링 기법은 패킷이 전송된 경로 정보를 확률 p로 샘플링하여 목적지에 전송하는 과정을 보인다.



[그림 3] 노드 샘플링 기반 PPM 기법

[그림 4]는 에지 샘플링 방법으로 라우터에서 자신의 IP 주소정보만을 패킷 헤더에 마킹하는 것이 아니라, 패킷이 전달된 앞단의 라우터 IP 주소정보까지도 같이 마킹하여 전달하는 방식이다. 이와 같은 노드 샘플링 기법은 해킹 공격 경로를 재구성하는 과정이 노드 샘플링 기법보다 뛰어나다.

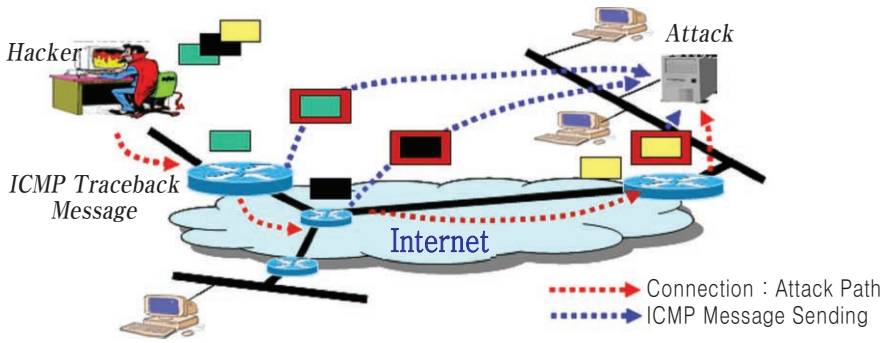


[그림 4] 에지 샘플링 기반 PPM 기법

변형된 PPM 기법으로는 라우터에서 마킹하는 패킷에 대한 인증 기능을 제공하여 마킹 과정에서 보안기능을 제공하는 방식 등이 있다.

(2) iTrace(ICMP Traceback) 역추적 기법

ICMP 역추적 기법은 PPM 기법과는 다른 접근 방법으로 수행된다. 라우터에서는 일반적으로 1/20,000의 확률로 패킷을 샘플링하여 iTrace 메시지를 생성하고 이를 패킷의 목적지 IP로 전송한다. iTrace 메시지는 일반적인 ICMP 메시지와 유사하게 이전 단계 라우터 정보와 다음 단계 라우터 정보를 포함하고 있으며 패킷의 Payload 정보 등을 포함하여 전달하게 된다. 생성시에 TTL(Time to Live) 필드 값은 255로 설정되어 전달되며 목적지에서는 TTL 값을 보고 네트워크 위상에서의 홉 거리 정보로 활용하여 공격경로의 재구성에 사용한다. iTraceback 기법에 대한 작동 방식은 **[그림 5]**와 같으나 일반적으로 PPM 기법과 마찬가지로 DDoS 공격에 대응하기 위해서는 상대적으로 많은 정보가 필요하기 때문에 개선된 기법의 연구가 필요하다.



[그림 5] ICMP Traceback 기법

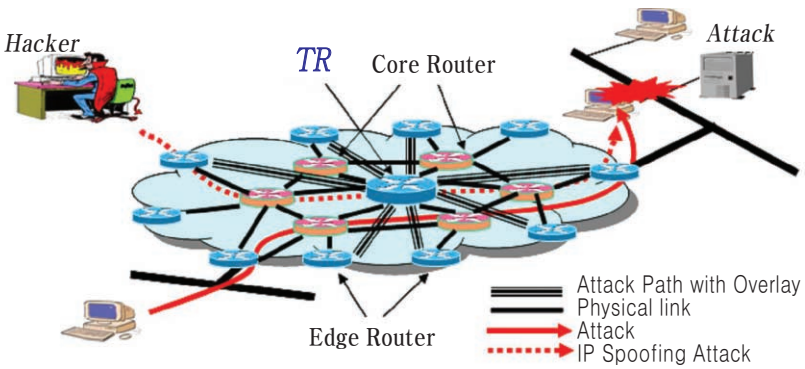
나. 대응적 역추적 기술

본 기술은 해킹 공격이 발생하였을 경우 피해 시스템에서 해킹 트래픽 연결에 대한 공격 경로를 홉 단계로 추적해 가는 방식이다. 구체적인 기법은 오버레이(Overlay) 네트워크 방식, 해쉬 기반 역추적 기술 및 IPSec 기반의 역추적 기법 등으로 나눌 수 있다.

(1) 오버레이 네트워크 기반 역추적 기법

본 기법은 역추적 라우터(TR : Tracking Router) 모듈을 네트워크에 별도로 설치하고 해킹 공격이 발생하였을 경우, 네트워크 위상에서의 종단 시스템과 연결된

라우터에서 전달된 정보를 TR로 전송한다([그림 6]). 즉, 기존의 Ingress 필터링 기법과 유사하게 종단 라우터에서 보내진 트래픽 정보는 터널링 방식으로 TR 라우터에 전달된다. 각 패킷에 대해 20 바이트 정보의 패킷 서명(Packet Signature) 정보를 생성하여 TR로 전달하게 된다. TR에서 수집된 패킷 관련 정보 등을 재구성하여 실제로 패킷이 전달된 경로를 분석하는 기법이지만, 네트워크 구성상 단일 TR로 전체 네트워크를 관리할 수 없기 때문에 소단위 네트워크에 적합한 기법이다. 또한 단일 ISP(Internet Service Provider) 네트워크상에서 구현 가능한 기법이며 이기종의 네트워크 환경에는 적용할 수 없다. 또한 해킹 공격은 짧은 기간 동안에 수행될 수도 있기 때문에 전체 경로를 역추적하는데 어려움이 발생할 수도 있으며, 공격자에 의해서 터널링된 패킷이 위조될 수도 있기 때문에 보안상의 문제가 발생하게 된다.

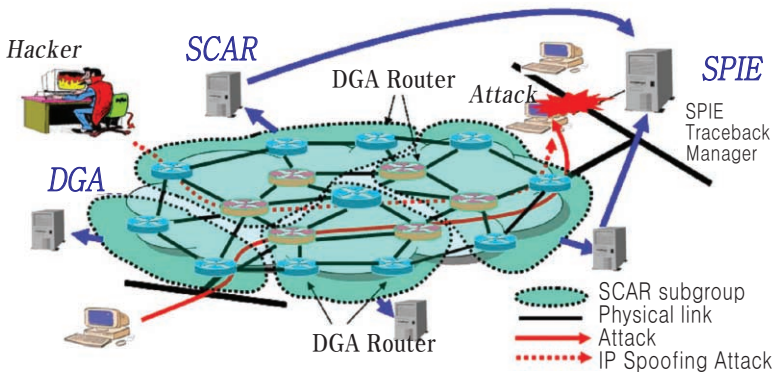


[그림 6] 오버레이 네트워크 기반 역추적

(2) 해쉬 기반 역추적 기법

본 기법은 SPIE(Source Path Isolation Engine) 기반 역추적 서버를 구성하고, 전체 네트워크를 서브 그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리한다.([그림 7]) 그리고, 각 라우터에는 DGA(Data Generation Agent) 기능을 탑재하여 운영한다. DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬값에 해당하는 IP 헤더 정보와 8 바이트 정보의 Payload 정보를 수집 관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 목적지 시스템에 있는 침입탐지 시스템에 의해 해킹을 발견하였을 경우 SPIE 시스템에서는 네트워크 그룹을 관리하는 SCAR(SPIE Collection and Reduction) 에이전트를 통해 그룹내 DGA 라

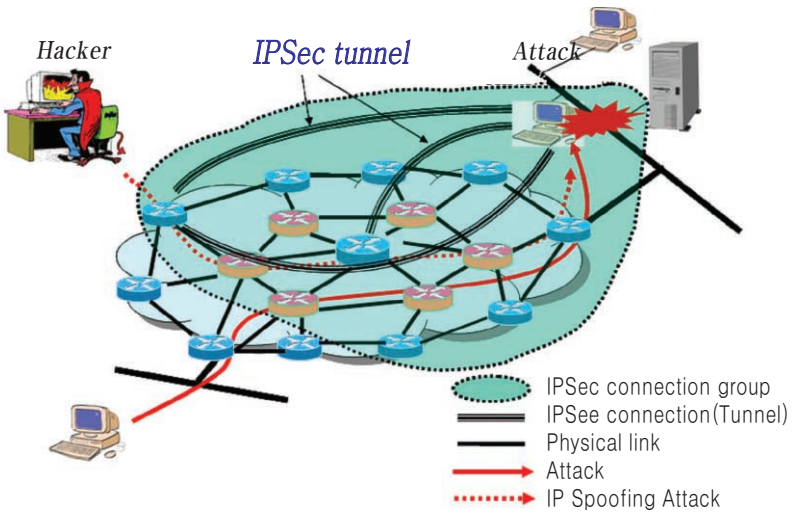
우터에 저장된 정보와 해킹 패킷 정보를 비교 분석하여 이를 다시 SPIE 시스템에 전달하게 되면 해킹 관련 패킷의 전송 경로를 재구성하게 된다. 본 기법을 적용하기 위해서는 SPIE, SCAR 및 DGA 기능을 구축하여야 하며 추가적인 모듈로 제공하기 때문에 이기종 환경의 ISP 간 적용도 가능하다. 실험 결과 0.5% 정도의 추가적인 해쉬 정보가 생성되어 전달되고 SCAR에서는 주기적으로 패킷에 대한 해쉬값을 관리하기 위한 메모리가 필요한 것으로 나타났다.



[그림 7] 해쉬 기반 역추적 기법

(3) IPSec 기반 역추적 기법

본 기법은 오버레이 네트워크 기반 역추적 기법에서 발생하는 터널링 과정에서의 보안상 취약점을 보완하기 위해 제시된 기법이다.([그림 8]) 전체 네트워크에 대한 위상을 각 라우터가 알고 있다는 가정하에 해킹 공격이 발생하게 되면 네트워크상의 라우터와 피해 시스템간에 IPSec 연결이 구성되어 공격자에 의한 공격 패킷이 해당 라우터를 통해 전달될 경우 IPSec 터널을 통해 경로 정보를 피해 시스템에 전달하게 된다. 다시 네트워크 위상에서의 주변 라우터를 선정하여 IPSec 터널을 구성하고 패킷에 대한 전송 여부를 판별하여 이를 피해 시스템에 전달하는 과정을 반복한다. 이와같은 과정을 통해 해킹 공격 발생시 실제적으로 패킷이 전송된 경로상의 라우터를 판별할 수 있게 된다. 물론 IPSec을 이용한 역추적 방식은 피해 시스템과 라우터 간에 IPSec 터널 연결을 구성한 경우에는 공격 경로를 파악할 수 있으나, IPSec 연결을 취하지 않은 네트워크에서는 경로 재구성에 어려움이 있다.



[그림 8] IPSec 기반 역추적 기법

다. 2003년 말까지의 공격근원지 역추적 기술 문제점

인터넷을 통한 해킹 공격에 대한 대응기술을 고찰할 때 우선 고려해야 하는 것은 인터넷 프로토콜 구조상 어느 계층을 중심으로 고찰할 것인가를 우선 결정해야 한다. 일반적으로 IP 계층에서의 역추적 기능을 제공하는 것이 일반적이며 TCP 계층인 경우 서비스 종류에 의존적이기 때문에 일반화하기에 어려움이 많이 있다. IP 계층에서의 역추적 기능을 제공하는 과정에서도 피해 시스템이 직접 모든 네트워크를 관리할 수 없기 때문에 결국에는 라우터에 의존하여 역추적 기능을 수행하게 된다.

(1) 전향적 역추적 기술에 대한 고찰

전향적인 기법인 경우 패킷을 중심으로 IP 헤더정보에 정보를 마킹하는 방식으로, 기존의 마킹 구조에서 유발하는 문제점을 해결할 수 있는 방안이 제시되어야 한다. 즉, 기존의 기법에서는 확률 p로 패킷을 선정하게 되는데 경로 재구성을 위해서는 상당히 많은 개수의 마킹된 패킷이 필요하다. 만일 특정 라우터에서의 에지 정보 또는 노드 정보 등이 마킹되지 않고 전달된다면 나머지 마킹된 정보를 가지고는 완벽한 공격 경로를 재구성할 수 없다는 문제점도 발견할 수 있으며, 최소한 하나의 노드 또는 에지 정보를 마킹하는데 알고리즘에서는 최소한 8개의 패킷을 선정하여 마킹해야 하기 때문에 전체적인 효율성 면에서도 비효율적이다.

iTrace 기법인 경우 기존의 패킷 정보에 대해 PPM과 마찬가지로 확률 p로 샘플링하여 메시지에 대한 iTrace 메시지를 생성하고 이를 목적지 IP로 전송하는 방식이다. 그러나, 현재 DDoS 공격 기법 중의 하나로 ICMP 기법을 이용한 방식이 발견되고 있어서 결국에는 iTrace 기법 역시 목적지 공격대상 시스템 측면에서 보았을 경우에는 또 다른 하나의 DDoS 공격으로도 보일 수 있기 때문에 이를 해결할 수 있는 방안이 필요하다.

이와같이 전향적 기법인 경우 패킷에 대해 일정 확률 p를 만족할 경우 샘플링하여 전송하는 기법을 사용하고 있는데, 이에 대한 구체적인 방안도 여러 가지를 생각할 수 있을 것이다. 만일 PPM 또는 iTrace 메시지를 발생하는 라우터에서 고정적인 형태의 확률 p에 의존하여 샘플링하지 않고 전체 네트워크의 트래픽 특성에 따라 능동적으로 확률 p를 조정할 수 있다면 기존 기법에 비해 네트워크 부하, 메모리 및 역추적 기능 등에서 보다 향상된 기법을 제공할 수 있을 것이다. 또한, 해커에 의한 오류 경로 재구성을 방지하기 위해서는 전통적인 보안구조를 역추적 모듈과 접목하여 제공한다면 더욱 개선된 기법을 제공할 수 있을 것이다.

(2) 대응적 역추적 기술에 대한 고찰

오버레이 네트워크를 이용한 역추적 기법인 경우 특정 네트워크 위상에만 적용가능하며 라우터의 구조가 동적으로 변화하는 일반적인 네트워크 환경에는 적용하기 어렵다. 또한, 종단 라우터가 아닌 망 내부 라우터에 연결된 라우터를 거쳐서 전달되는 패킷인 경우 쉽게 추적할 수 없다는 문제점이 발생한다.

해쉬 기반 역추적 기법인 경우 패킷에 대한 해쉬값을 일정한 주기로 관리 전송하는 방식이지만 네트워크가 규모가 방대한 경우 전체 성능에 많은 문제점이 발생하게 된다. 또한 침입탐지시스템 등을 통해 해킹 등이 발견된 경우에 역추적 과정을 수행하는 방식이므로 우선 네트워크 자체에 대한 공격이 수행된다면 본 기법 역시 작동하지 않는다는 문제점이 있다.

IPSec에 기반한 역추적 기법인 경우 우선 공격자는 IPSec이 가지고 있는 보안 및 인증 특성에 의해서 DDoS 및 인터넷 웜 공격을 수행하지는 않을 것이며 일반 네트워크 환경에서 해킹 공격을 수행할 것이다. 따라서 IPSec 기법을 적용한다는