情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

# 역추적 기술 및 보안 요구사항 분석

한 정 화*, 김 락 현**, 류 재 철***, 염 흥 열****

요 약

최근 인터넷의 급속한 발전을 기반으로 국경을 초월하여 인터넷을 이용한 각종 해킹, 사이버 공격 및 범죄가 기하급수적으로 증가하고 있다. 이와 같은 상황에서 각종 침해사고로부터 시스템, 네트워크 및 중요한 정보를 보호하기 위한 다양한 보안 강화 시스템이 개발되어 적용 운용되고 있지만, 현재 적용되어 사용되고 있는 보안 강화 시스템들은 해킹, 공격 및 범죄가 발생된 후 이를 막기 위한 방법으로 수동적인 기능으로 사용되고 있다. 그 결과 해킹, 사이버 공격 및 범죄를 사전에 미리 방지하는 데는 한계를 갖고 있는 것이 사실이다. 때문에, 현재 역추적 분야에서는 해킹, 사이버 공격 및 범죄가 발생할 경우 능동적이고 실시간으로 빠른 추적이 가능한 보안 강화 시스템을 목표로 하는 연구가 진행되고 있다. 이에 본 논문에서는 TCP/IP 기반의 다양한 역추적 기술을 각각 분석하고 역추적 기술을 발전시키기 위한 요구사항을 분석하여 연구동향에 관하여 살펴보고자 한다. 본 논문은 참고문헌 [16]의 결과를 활용해 작성했으나, 표준화 동향과 요구사항, 요구사항에 근거한 기존 방식들의 특징을 제시하였다.

## Ⅰ. 서 론

인터넷의 급속한 발전을 기반으로 우리 일상생활은 많은 변화를 가져왔다. 통신, 정보 수집, 멀티미디어, 화상회의 등 열거할 수 없을 정도로 인터넷은 다양한 매체로 사용되며 사용의 편리함 때문에 사용자 또한 기하급수적으로 증가하고 있다. 이와 같이 인터넷과 같은 네트워크의 발전은 편리함, 정보교류 라는 순기능에 반해 네트워크를 통한 시스템 해킹 및 정보유출, 불법 침입 그리고 악성 바이러스 유포 등의 역기능과 같이 인터넷 사용자와 사용량의 증가와 더불어 인터넷을 이용한 각종 침해 공격 역시 크게 증가하고 있는 것이 사실이다. US-CERT (United States Computer Emergency Readiness Team)에서 발표한 자료에 따르면 매년 인터넷을 이용한 공격은 측정 불가능할 정도로 급성장하고 있고,[1] 이에, 정보보호 전문가 및 업체는 다양한 방법으로 인터넷을 이용한 공격에 대응하기 위하여 많은 연구를 진행하고 있다.

역추적 기술은 인터넷을 통한 각종 침해 공격의 증가와 은폐 및 위장, 위조 기법의 향상, 공격 후 남아있는 로그분석을 통한 역추적의 한계, 다국을 경유한 해외 프락시 서버 경유 및 IP 스푸핑 등 공격 시 추적의 불가능 때문에 개발 연구 되었다. 또한 역추적을 기반으로 사이버 범죄에서 법률적 근거(Forensics)를 강화하고 책임 소재 규명 및 처벌, 재 침입 방지와 같은 효과를 얻을 수 있기 때문에, 해커의 해킹 시도 자체를 제한할 수 있는 해킹 방지 시스템을 개발하고자 하는 노력이 시도되고 있다. 그러나 현재 인터넷상에서 동작하는 여러 보안 강화 시스템들은 매우 다양하고 해커의 해킹에 대한 상호 협력을 통한 대응이 거의 불가능한 상황이므로, 이와 같은 보안 시스템 환경은 효과적으로 방어하지 못하는 것이 현실이다. 이에 해킹 방지를 위해 가장 효과적이고 더욱 효율적인 방법의 역추적 시스템에 대한 연구가 활발히 진행되고 있다. 그리고 최근 ITU-T SG17 9월 회의에서 2010년까지 역추적에 대한 표준화 작업을 진행하기로 하였다. ITU에서 역추적에 대한 표준화 작업을 진행함으로써 앞으로 역추적에 대한 연구 또한 활발히 진행될 것으로 예상된다.

"본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음"
(IITA-2008-C1090-0801-0016), 단, 저자중 염흥열은 이 지원사업에 참가하지 않았음

* 순천향대학교 정보보호학과 (jhhan@sch.ac.kr)
** 순천향대학교 정보보호학과 (rhkim@sch.ac.kr)
*** 충남대학교 정보통신공학부 (jcryou@home.cnu.ac.kr)
**** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

본 논문에서는 현재 진행되고 있는 TCP/IP 역추적 기술 연구의 동향에 대하여 살펴보고, 역추적 기술에 대해 알아보고자 한다. 또한 역추적에 대한 표준화 진행 현황을 알아보고, 역추적 기술을 발전시키기 위해 만족해야하는 요구사항들을 분석하여 역추적 발전 방향에 대해 살펴보고자 한다.

본 논문의 구성은 2장에서 역추적에 대한 개념과 구분에 대해 알아보고, 3장에서는 현재 발표된 TCP 역추적 기법에 관해 알아본다. 4장에서는 IP 기반의 역추적 기법에 관해 살펴보고, 5장에서는 역추적을 위한 요구사항과 표준화 현황에 대해 알아본 후, 6장에서는 앞 서 알아본 역추적기법과 요구 사항을 비교 분석한다. 마지막으로, 6장에서는 결론 및 향후 역추적 연구 방향에 대해 정의해 보고자 한다.

## Ⅱ. 역추적 (Traceback)

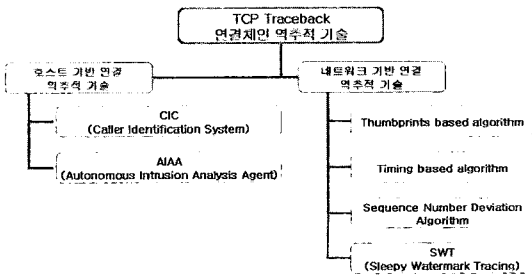
역추적(Traceback)은 통신망(인터넷)을 이용하여 공격(해킹)을 시도하는 공격자(해커)의 위치를 실시간으로 분석하고 추적하는 기술을 말한다. 역추적은 통신 환경과 연결 방법에 따라 다양한 방법이 존재하며, 각 역추적 방법에 따라 다양한 기법이 적용된다.

### 2.1 역추적 기술의 분류

역추적 기법은 연결 방법, 대응 방식, 적용 기법에 따라 분류할 수 있다.

(1) 연결 방법에 따른 분류

TCP 연결 역추적과 IP 역추적으로 구분할 수 있다. TCP 연결 역추적은 TCP 통신 방식의 특성을 이용하여 연결 지향성 통신 방식에서 사용되는 역추적 방식이다. 이 방식은 주로 연결체인의 특성을 이용하여 역추적 한다. 반면 IP 역추적 기법은 비 연결지향성 통신 방식을 이용하기 때문에 공격을 당한 시스템에 남겨진 로그를 분석하여 그 흔적으로 공격자의 위치를 추적한다.



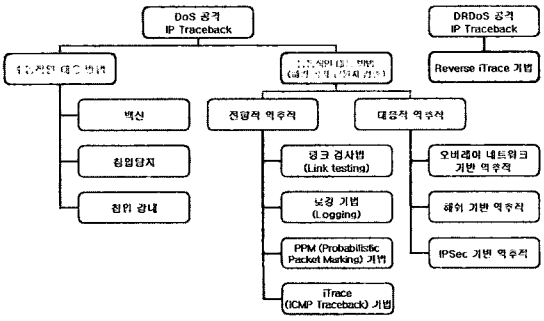

〔그림 1〕 TCP 연결 역추적 방식

(2) 대응 방식에 따른 분류

공격을 당한 피해 시스템에 남겨진 흔적을 이용하여 공격자의 위치를 추적하는 수동적인 방법의 역추적 방식과 해킹 시도 자체를 제한할 수 있는 능동적인 해킹 방어를 하는 능동적인 방법으로 분류할 수 있다. 현재 많은 학자들과 업체에서는 실시간으로 공격 시도 자체를 제한, 차단할 수 있는 능동적인 공격 방지 시스템 개발에 온 힘을 쏟고 있다.

(3) 적용 기법에 따른 분류

통신에 참여하는 참여자의 시스템 중 어떤 위치에 역추적 모듈을 탑재 하는가에 따라 네트워크 기반 역추적 방식과 호스트 기반 역추적 방식으로 구분한다. 네트워크 기반 역추적 방식은 네트워크를 연결하거나 제어하는 장비, 즉 서버, 라우터 게이트웨이 등에 역추적 모듈을 설치하여 네트워크를 통과한 데이터(제어 및 사용자 데이터 및 헤더)로부터 정보를 구하여 역추적하는 방식이고, 호스트 기반 역추적 방식은 통신에 참여한 네트워크 내의 호스트에 역추적 모듈을 설치하여 그 정보를 이용하여 역추적 하는 방식이다. 각 역추적 방식은 네트워크 환경과 운영 방식에 따라 장/단점이 존재하며, 이를 보완한 새로운 역추적 방식의 개발이 최우선이 되어야 한다. 다음 [그림 1]과 [그림 2]는 TCP 역추적 방식과 IP 역추적 방식을 구분한 것이다. IP 역추적 방식은




〔그림 2〕 IP 역추적 방식

DoS 공격에 대한 역추적 방식과 DRDoS 공격에 대한 역추적 방식을 구분하여 도시 하였다.

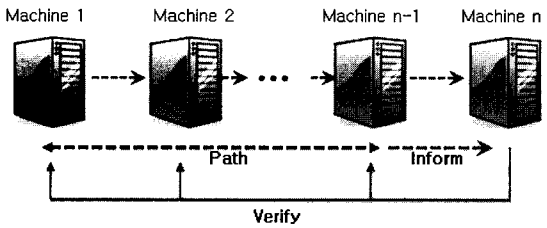
## Ⅲ. TCP 역추적 기법

TCP 역추적 기술은 공격자가 우회공격을 시도하는 경우에 공격자의 실제 위치를 추적하는 기술이다. TCP 연결은 개념적으로 연결지향성과 신뢰성 기반 연결을 갖는다. 그렇기 때문에 공격자는 자신의 위치를 바로 드러내지 않기 위해 우회공격을 이용한다. 우회공격이란 공격자가 공격 대상자의 컴퓨터를 바로 공격하지 않고, 다수의 중간 경유지(호스트)를 이용하여 경유한 후 최종적으로 공격 대상자의 컴퓨터에 공격을 시도하는 것이다. 우회공격을 이용할 경우, 피해자의 컴퓨터에서 공격자의 위치를 최종 경유한 호스트로 잘못 판단하게 할 수 있다. 때문에, TCP 역추적에서 역추적을 위해 사용하는 개념으로서 연결 체인을 이용한다. 연결 체인은 공격자가 다수의 경유 호스트를 거쳐 공격을 시도할 경우, 공격 호스트로부터 최종 공격 대상 호스트 사이에 TCP 통신을 위한 연결 체인이 형성되어 이를 이용한다는 원리이다. 또한 연결 체인이 형성될 경우, 네트워크 또는 호스트들은 연결 체인을 관리할 보안 모듈을 탑재하고 있어야 한다. 이에 관리 모듈의 탑재 여부에 따라 TCP 역추적 기술을 네트워크 기반 연결 역추적과 호스트 기반 연결 역추적 기술로 구분하기도 한다.

### 3.1 호스트 기반 연결 역추적 기법

#### 3.1.1 CIS(Caller Identification System)

CIS[2]는 사용자가 특정 시스템에 접속 요청을 할 때, 이 접속 요청이 정당한지 확인하여 접속 허용의 유무를 판단함으로써 안전한 연결체인을 구성하는 기술이다. 접속을 요청하는 시스템은 특정 시스템에 접속하기위해

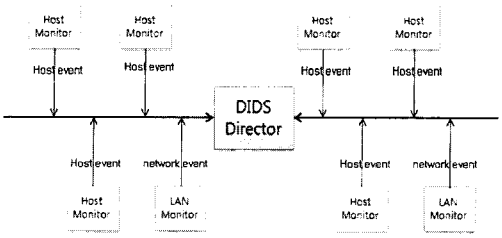



〔그림 3〕 CIS 연결체인 구성

자신이 경유해온 모든 시스템들의 정보를 그 시스템에 제공한다. 접속 요청을 받은 시스템은 이 목록을 바탕으로 경유 시스템들의 정보가 정당한지 확인하게 되고, 이러한 목록이 유효할 때만 접속을 허용하여 연결체인을 구성한다.

#### 3.1.2 DIDS(Distributed Intrusion Detection System)

DIDS[3]는 다수의 호스트와 네트워크로부터 데이터를 수집하여 침입을 탐지하는 시스템으로 DIDS는 Director, Host monitor, LAN monitor로 구성된다. Host monitor에서는 호스트들의 감사 자료를 수집하고, LAN monitor에서는 네트워크 트래픽을 모니터하여 두 monitor에서 수집한 정보들을 DIDS Director에게 보내준다. 여기서 접속이 모니터 되는 환경에 처음 들어갈 때 네트워크 사용자 식별자인 NID(Network Identification)를 생성하여 익명의 다수의 사용자 인증으로 인한 문제들을 해결하며 역추적에 이용할 수 있다.

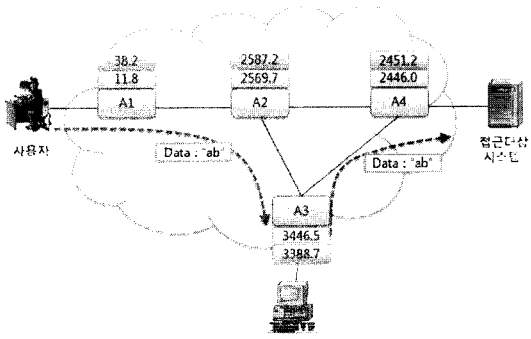



〔그림 4〕 DIDS 구성

### 3.2 네트워크 기반 연결 역추적 기법

#### 3.2.1 Thumbprints based algorithm

Thumbprint를 이용한 역추적[4] 방법은 Thumbprint 알고리즘을 이용하여 공격자에서 공격 대상시스템까지의 연결체인을 구성하여 역추적하는 방법이다. 하나의 연결체인에 송·수신되는 데이터의 내용은 동일하므로 데이터의 정보를 요약한 thumbprint값 또한 동일하다. 연결체인에 속한 각 시스템에서는 thumbprint값으로 보통 위치 정보를 포함하는 벡터값으로 추출하여 저장한다. 동일시간에 같은 연결체인을 구성하는 각 연결의 thumbprint를 비교하여 근원지를 역추적 할 수 있다. [그림 5]와 같이 네트워크 시스템에 첫 번째로 저장된




〔그림 5〕 Thumbprint를 이용한 연결체인 구성

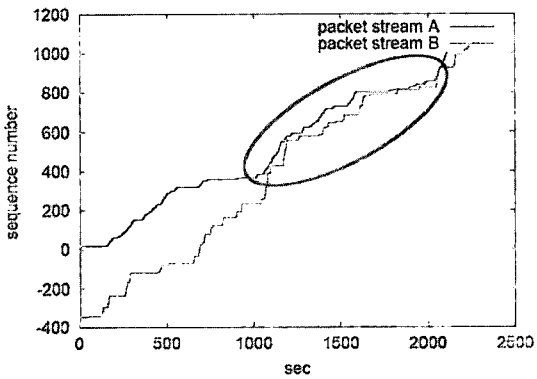
thumbprint들의 값과 두 번째로 저장된 thumbprint들의 값의 각각의 합이 비슷하며, 이 thumbprint값의 합이 비슷함에 따라 두 연결이 동일한 연결체인임을 확인 할 수 있다.

### 3.2.2 TCP sequence number algorithm

TCP sequence number 알고리즘[5]을 이용한 역추적은 패킷의 IP, TCP 헤더, time stamp를 이용한 네트워크 기반의 역추적으로, Data의 정보를 이용하여 Thumbprint에 반해 sequence number에 따른 데이터의 양이 크게 변하지 않는다는 점을 이용하여 연결체인을 구성하는 방법이다.

보통 인터넷 백본 네트워크의 트래픽 포인트에서 패킷을 캡처하여 패킷의 IP주소, TCP헤더, 타임스탬프를 수집한다.

IP주소와 TCP헤더의 포트번호를 이용하여 패킷 스트림(업 스트림, 다운스트림)을 구분한다. 동일한 두 패킷 스트림이 같은 연결체인에 속하면 [그림 6]과 같이




〔그림 6〕 두 연결의 패킷 스트림 증가 그래프

송·수신되는 데이터의 Sequence Number 증가 정도는 비슷하다. 이와 같은 방법으로 각 연결의 패킷 스트림은 타임스탬프와 시퀀스 번호에 대한 편차를 이용하여 공격 경로를 역추적 한다.

## Ⅳ. IP역추적 기법

IP 역추적 기술은 해킹 공격에 대해 스푸핑된 공격 패킷의 근원지 IP를 역추적 할 수 있는 기술로써, IP역추적을 위해 공격 경로와 패킷의 송신자를 추적하여 Attack Graph를 재구성한다. 대표적인 기법으로는 패킷을 중심으로 마킹 방법론을 사용한 기법, ICMP 프로토콜과 같은 프로토콜 등에 대한 변형을 통해 근원지 패킷의 전달 경로 정보를 관리하는 기법 그리고 네트워크 망 구조 측면에서 관리 프로토콜을 이용하는 방법 등이 있다. 각각의 기법은 인터넷 환경에서 DoS 및 DDoS 공격에 장단점을 가지고 있으며, 적용 방법 및 해킹 공격의 특성에 따라서 각기 다른 성능을 보인다.

### 4.1 Proactive tracing

네트워크상에 패킷이 전송되는 과정에서 사전에 역추적 경로 정보를 생성하여 이를 패킷에 삽입하여 목적지로 전달하는 방법으로, 주기적인 관리 하에 해킹 공격이 발생했을 때, 이미 전송된 역추적 정보를 분석하여 해킹 공격의 근원지를 찾는 기법이다.

#### 4.1.1 링크 검사법

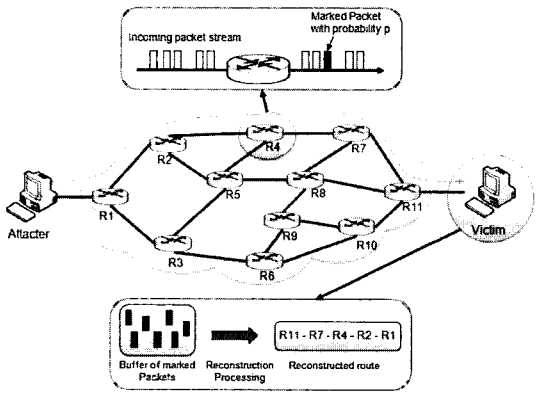
링크 검사법은 Hop-by-Hop 추적 방식에 해당하는 역추적 방법이다. 패킷의 정보를 기반으로 하여 각 라우터에 연결된 링크를 검사하여 연결의 근원지를 추적하는 기본적인 역추적 방법이다.

#### 4.1.2 로깅 기법

로깅 기법[6]은 라우터로부터 전송된 패킷의 특성 등을 기록해 놓은 후, 패킷을 보낸 근원지를 추론하는 시스템에 적용하여 역추적하는 기법이다. 많은 양의 데이터를 저장하여 추론하기 때문에 확률적인 샘플링 기법과 필터 기법 등을 적용하여 처리 데이터의 양을 줄여 추론 과정을 간략하게 한다.

#### 4.1.3 PPM(Probabilistic Packet Marking)기법

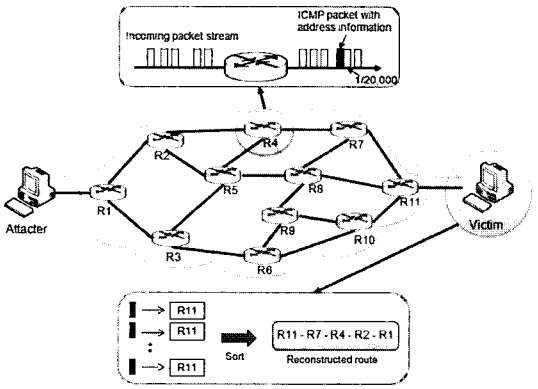
PPM[8]은 네트워크를 구성하는 라우터에서 자신을 지나는 패킷에 라우터 정보를 삽입하여 스푸핑된 패킷의 실제 경로를 찾는 방법으로, 라우터에서는 패킷IP 헤더에 자신의 IP 주소를 마킹하여 다음 라우터에 전송한다. 라우터에는 많은 패킷이 지나가기 때문에 일정한 확률 p로 패킷을 샘플링하는 노드 샘플링(Node sampling), 에지 샘플링(Edge Sampling)등을 이용하여 네트워크 상태를 유지한다. 마킹된 패킷을 받은 후, 시스템이 공격을 받게 되면 수집된 패킷의 헤더 정보를 가지고 공격경로를 재구성하여 공격자의 위치를 추적한다.




〔그림 7〕 PPM 역추적[7]

#### 4.1.4 iTrace(ICMP Traceback)기법

iTrace[9]는 라우터에서 일정한 확률로 패킷을 샘플링한 후, iTrace 메시지를 생성하여 샘플링한 패킷과 함께 목적지로 전송한다. iTrace 메시지는 ICMP 패킷의 message body에 역추적 정보를 입력한 메시지이다. iTrace 메시지를 생성할 때 초기 TTL(Time To Live) 필드 값은 255로 설정되어 전달된다. iTrace 메시지를 받은 시스템은 공격이 발생하면 라우터가 생성한 iTrace 메시지의 TTL 값을 확인하여 홉 단위로 공격경로를 추적한다.



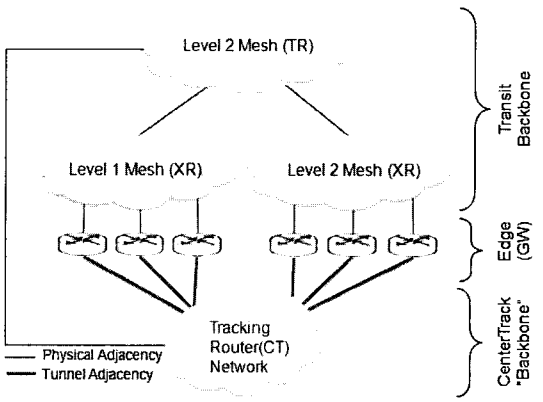

〔그림 8〕 iTrace 역추적[7]

### 4.2 Reactive Tracing

해킹 시도가 발견되면 연결되어있는 상태에서 공격경로를 홉 단계로 추적해 공격 근원지를 추적해 가는 방식이다.

#### 4.2.1 오버레이 네트워크 기반 역추적

오버레이 네트워크(Overlay network) 기반 역추적[10]은 역추적 라우터(TR : Tracking router)모듈을 네트워크에 설치해야한다. TR을 설치한 후 공격이 발생하면, 피해 시스템과 이 시스템과 연결된 라우터는 공격 패킷의 정보를 TR에 전송한다. TR는 수집된 패킷 정보를 이용하여 공격경로를 분석하게 된다.




〔그림 9〕 오버레이 네트워크 구성

#### 4.2.2 해쉬기반 역추적 기법

Hash 기반 역추적 기법[11]은 SPIE 역추적 관리 시스템을 중심으로 두어 네트워크 내에 서브그룹을 구성하여 네트워크를 관리한다. 서브그룹의 각 라우터에는 DGA(Data Generation Agent)를 설치하여 해당 라우터

를 거치는 패킷의 정보(IP헤더, 8바이트 페이로드)를 Bloom Filter를 적용한 결과를 digest table에 저장한다.

공격에 대한 역추적 요청 시, SPIE는 각 서브그룹을 관리하는 STM(SPIE Traceback Manager)에게 패킷 정보를 요청하며, STM은 DGA에 저장된 패킷 정보와 공격 패킷 정보를 비교하여 SPIE 시스템에게 전달한다. SPIE 시스템은 받은 공격에 관련된 패킷의 전송 경로를 재구성하여 근원지를 추적 한다.

#### 4.2.3 IPSec 기반 역추적

IPSec 기반의 역추적 기법[12]은 오버레이 네트워크 기반 역추적 기법에서 공격자가 터널링 과정에서 거짓 정보를 보낼 수 있는 취약점에 대해 제시된 기법이다. 우선, 이 기법은 네트워크에 대한 위상을 각 라우터가 알고 있다는 전제하에 동작한다. 시스템이 공격을 받으면, 이웃 라우터와 피해 시스템간에 IPSec 연결을 구성한다. IPSec 터널 연결을 한 라우터에 공격 패킷이 지나가면, IPSec 연결을 통해 피해 시스템에 공격정보를 보낸다. 해당 라우터들을 대상으로 이 과정을 반복하고 반복된 과정을 통해 공격 패킷의 전송경로를 수집하고 분석하여 공격 경로를 재구성한다.

## V. 역추적을 위한 요구사항 및 표준화 현황

이 절에서는 효율적인 역추적 기술을 개발하기위해, 역추적 기술이 만족해야하는 요구사항들에 대해 알아본다.

### 5.1 역추적을 위한 일반적인 요구사항

역추적 기술에 대한 일반적인 요구사항은 다음과 같다.[13]

- 호환성 : 역추적 프로토콜은 현재 존재하는 프로토콜이 하드웨어와 소프트웨어를 포함하는 NGN 구조와 호환되어야 한다.
- 작은 네트워크 트래픽 오버헤드 : 역추적 메커니즘은 네트워크 트래픽이 현저하게 증가하지 않아야한다.
- 복잡성에 대한 충돌 최소화 : 역추적 메커니즘은 점차 증가하는 동작에 반하여, 복잡성에 따른 충돌을 최소화시켜야 한다.
- 견고성 : 역추적 메커니즘은 DDoS 공격에 매우 효과적이며 튼튼해야 한다.
- 시간과 자원사이의 오버헤드 최소화 : 역추적 메커니즘은 시간과 자원 사이의 오버헤드 충돌을 최소화해야한다.
- 역추적 기능의 부분적 배치 : 역추적 메커니즘은 상대 라우터를 네트워크의 일부분만 배치한 경우에도 동작해야한다.
- 변화 최소화 : 역추적 메커니즘은 라우터에 변화를 작게 요구해 한다.
- 적은 패킷 요구 : 역추적 메커니즘은 피해자가 적은 패킷만으로도 공격 경로를 식별할 수 있도록 허용해야 한다.
- 확장성 : 역추적 메커니즘의 크기는 정확성(false positives, false negatives 측정)을 유지하는 한 많은 공격자들에 비례해야 한다.
- Locality : 역추적 메커니즘은 공격 피해자가 어떠한 라우터 또는 ISP와 통신없이도 위치적 역추적을 수행하도록 허용해야한다.
- 멀티-도메인 역추적 : 역추적 메커니즘은 다른 도메인에 존재하는 공격자를 식별해야한다.

### 5.2 역추적을 위한 세부 요구사항

ITU-T SG17 표준화 회의에서 합의된 역추적에 대한 세부적인 요구사항은 다음과 같다.[14]

(1) 역추적 서비스에서, 네트워크 이벤트의 요구사항을 실시간으로 처리하기 위해 역추적 응답 시간이 필요하다.
(2) 역추적 메커니즘은 이벤트의 특징에 기반하는 네트워크 이벤트의 근원지를 결정할 수 있어야 한다. 예를 들면, 트래픽 특징으로 DDoS 근원지를 결정할 수 있어야 한다.
(3) 역추적 메커니즘은 이벤트의 단일 패킷에 기반을 두는 네트워크 이벤트의 근원지를 결정할 수 있어야 한다.
(4) 역추적 메커니즘은 스푸프된 패킷의 발신자를 결정할 수 있어야 한다.
(5) 역추적 메커니즘은 다른 도메인들 간에 전송되는 패킷의 발신자를 결정할 수 있어야 한다.
(6) 응용 계층 라우트가 존재한다면, 역추적 메커니즘은 응용 계층 라우트에서 그 엔티티의 정보를

확인할 수 있어야 한다. 메일 서비스에서 예를 들면, 역추적 메커니즘은 받은 메일을 기반으로 첫 번째 전송 메일 서버를 확인할 수 있어야 한다.

(7) 역추적 메커니즘은 네트워크 계층 경로에 존재하는 엔티티들의 정보를 확인할 수 있어야 하며, 특히 첫 번째 엔티티의 정보를 확인 할 수 있어야 한다. 예를 들면, 수신 받은 패킷에 기반을 두는 역추적 메커니즘에 의해 ingress 라우터를 찾아낸다.

(8) 역추적 메커니즘은 IP 주소가 사용 될 때, 이것의 IP 주소와 시간에 기반을 둔 네트워크 엔티티의 지리적 정보(건물 주소)와 논리적인 네트워크 위치 정보(확실한 네트워크 기사의 도메인 위치 주소)를 확인 할 수 있어야 한다.

### 5.3 ITU-T 표준화 추진 현황

2008년 4월, ITU-T SG17 회의에 중국에서 새로운 표준화 항목으로 역추적을 제안하여 채택되었다. 이에, CBS 인터넷 뉴스[15]에서는 ITU에서 역추적 기술을 마련함에 따라 이것이 온라인상의 익명성을 제한하여 개인의 프라이버시를 침해할 것이라는 우려를 보도하여 역추적 기술 연구에 대한 관심도 높아지고 있다.

최근 ITU-T SG17 9월 회의에서는 역추적 표준화 작업을 위한 기본 틀을 정하고, 2010년까지 SG17 Q6에서 표준화 작업을 진행하기로 하였다.

## Ⅵ. 역추적 분석

이 절에서는 기존의 역추적기법들이 앞에서 알아본 요구사항을 만족하는지 비교, 분석한다. 역추적 기법을 분석하기 위한 요구사항 항목들은 다음과 같다.

① 실시간으로 역추적 가능해야 한다.
② 트래픽의 특징을 이용한 역추적이 가능해야 한다..
③ 샘플링한 패킷을 기반으로 역추적이 가능해야한다.
④ IP위조패킷을 보낸 근원지를 추적할 수 있어야한다.
⑤ 다른 네트워크에서 전송되는 패킷의 근원지를 추적할 수 있어야 한다.
⑥ 응용 서비스에서 제공하는 정보를 이용하여 서비스를 제공하는 서버의 위치를 추적할 수 있어야 한다.
⑦ 수신 받은 패킷의 정보를 이용하여 패킷 전송이 시작된 네트워크 시스템의 위치를 추적할 수 있어야한다.
⑧ IP주소와 시간을 이용하여 네트워크의 위치 정보를 확인할 수 있어야 한다.

다음은 역추적 요구사항들과 TCP, IP역추적 기술들을 분석한 [표 1]에 대한 설명이다.

① : TCP 역추적 기법들은 TCP 연결 세션이 성립한 상태에서 역추적을 수행하므로 실시간 역추적이 가능하다. 그리고 Hash기반 역추적, IPSec기반 역추적, overlay네트워크 기반 역추적 기법은 통신이 연결되어 있는 상태에서 바로 역추적이 가능하지만, 나머지 Proactive 역추적 기술들은 이미 전송된 정보들을 분석하여 근원지를 찾으므로 실시간으로 역추적하기 힘들다.

② : IP역추적 기법들은 패킷기반의 역추적으로 패킷

〔표 1〕 역추적 기본 요구사항과 TCP, IP 역추적 기술 분석 (○:해당됨, ×:해당되지 않음)

| 분류 | 기법 | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ⑧ |
|---|---|---|---|---|---|---|---|---|---|
| TCP | CIS | ○ | × | × | ○ | × | × | × | × |
| | DIDS | ○ | × | × | ○ | × | × | × | × |
| | Thumbprint | ○ | × | × | ○ | × | × | × | × |
| | Squence | ○ | × | × | ○ | × | × | × | × |
| IP | Link Test | × | ○ | × | × | ○ | × | × | × |
| | Logging | × | ○ | × | × | ○ | × | × | × |
| | PPM | × | ○ | ○ | × | × | × | ○ | × |
| | iTrace | × | ○ | ○ | × | × | × | ○ | × |
| | Hash TB | ○ | ○ | × | × | × | × | ○ | × |
| | IPSec TB | ○ | ○ | × | ○ | × | × | ○ | × |
| | overlay TB | ○ | ○ | × | × | × | × | ○ | × |

의 특징을 이용하여 역추적 하므로 이 항목을 만족한다.

③ : 패킷기반의 역추적 기법은 IP 역추적에 해당하며, PPM과 iTrace 기법은 라우터를 지나는 패킷을 확률적으로 샘플링하여 역추적에 이용하므로 이 항목을 만족한다.

④ : TCP 역추적 기법들은 TCP 연결체인에 기반하여 역추적을 수행하므로 IP가 위조되어도 역추적이 가능하다. 반대로, IP역추적 기법들은 패킷의 IP를 기반으로 역추적을 수행하므로 IP가 위조되면 역추적하기가 어려우나 IPSec을 이용한 역추적 방법은 IPSec으로 안전한 통신 터널을 생성하여 통신하므로 IP의 주소가 위조되어도 역추적이 가능하다.

⑤ : Link test와 Logging 기법은 역추적을 위한 패킷에 어떠한 수정을 하지 않기 때문에 역추적 모듈을 설치하지 않은 네트워크의 시스템과 통신하는 패킷들의 근원지를 추적할 수 있다.

⑥ : 위에서 알아본 기존의 역추적 기법들은 네트워크 계층에서 동작하므로 이 항목에 해당하지 않는다.

⑦ : 패킷기반으로 동작하는 IP역추적 기법 중에서 PPM, iTrace, Hash기반의 역추적, IPSec을 이용한 역추적, overlay 네트워크기반의 역추적 기법들이 이 항목에 해당되며, 모두 패킷이 지나온 경로에 대한 정보를 갖고 역추적 하므로 네트워크상의 패킷 근원지를 추적할 수 있다.

⑧ : 위의 IP역추적 기법들은 IP 주소를 이용하여 패킷의 네트워크 근원지를 추적하지만, IP 주소와 패킷을 사용한 시간으로 논리적인 위치 정보를 찾아내지 않는다.

## Ⅶ. 결론 및 향후 과제

통신 네트워크에서 발생되는 다양한 공격에 대비하기 위한 연구 중에 하나로 역추적 기술이 있으며, 많은 연구자들에 의해 역추적 기술들이 개발되었다.

이에 본 논문에서는 역추적 기술의 개념과 동작에 대해 알아보고, 주요한 역추적 기술들과 역추적 기술이 만족해야하는 요구사항들에 대해 알아보았다. 또한 이러한 과정을 바탕으로 역추적 기술과 역추적 기술에 대한 요구사항들을 비교 분석하였다.

Ⅵ장에서 역추적 기술들을 분석한 결과, 기존의 역추적 기술 중에 IP 연결 역추적 기법들이 TCP 연결 역추적 기법들보다 요구사항을 더 만족하였지만, 역추적 기술이 갖춰야할 요구사항의 대부분을 만족하지 않았다.

기존의 역추적 기술들은 실제 네트워크 환경에서 실용하지를 못하는 문제점을 갖고 있었다. 따라서, 모든 네트워크에 적용 가능한 역추적을 개발하기 위해서는 역추적 기술을 개발하기위한 요구사항을 표준화하여 그 요구사항을 만족하는 역추적 기법을 연구 및 개발해야 할 것이다.

## 참고문헌


[1] US-SERT, http://www.us-cert.gov/

[2] H.T. Kulin, H.L. Kim, Y.M. Seo, G. Cheo, S.L. Min, C.S. Kim, "Caller Identification System in the Internet Environment," *Proc. of the USENIX Security 4th Symposium*, 1993.

[3] Steven R. Snapp, James Brentano, Gihan V. Dias, "DIDS(Distributed intrusion Detection System) - Motivation, Architecture, and An Early Prototype," *Proc. of the 14th National Computer Security Conference*, 1991.

[4] S. Staniford-Chen and L.T. Heberlein, "Holding intruders accountable on the internet," *In Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 39-49, 1995.

[5] K. Yoda and H. Etoh. "Finding a Connection Chain for Tracing Intruders," *6th European Symposium on Research in Computer Security - ESORICS 2000th*, pp. 191-205, 2000.

[6] S. Stenfan, W. Dwetherall, "Network Support for IP Traceback," *IEEE/ACM Transactions on networking*, Vol. 9, No.3, June 2001.

[7] 허준, 강명수, 홍충선, "IPv6 네트워크 환경에서의 경량화된 IP 역추적 기법", *한국정보보호학회 논문지*, pp. 93-102, 2007.

[8] D.X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Tracebackm," *In Proc. of IEEE INFOCOM Conference*, 2001.

[9] Steve Bellovin, Marcus Leech, Tom Taylor, "ICMP Traceback Messages," IETF, draft-ietf-itrace-04,

Feb. 2003.

[10] R. Stone, "Centertrack : An IP Overlay Network for Tracking DoS Floods," *Proc. of 9th USENIX Security Symposium, Denver, Colorado*, pp. 199-212, August, 2000.

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

[12] H.Y. Chang, R Narayan, S.F. Wu, B.M. Vetter, X. Wang, M. Brown, J.J. Yuill, C. Sargor, F. Jou, F. Gong, "Deciduous : Decentralized Source Identification for Network-based Intrusions," *6th IFIP/IEEE International Symposium on Integrated Network Management*, 1999.

[13] Stefan Savage, David Wtherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback," *Proc. Of ACM SIGCOMM 2000*, pp. 295-306, 2000.

[14] Tian Huirong, Richard Brackney, H. Y. Youm, "Draft text of Rec. X.tb-ucr: Traceback Use Cases and Capabilities", TD4158, ITU-T SG17, Sep. 2008.

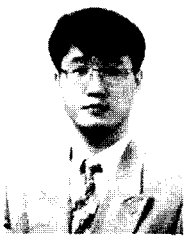
[15] U.N. Agency Eyes Web Anonymity Controls, http://www.cbsnews.com/stories/2008/09/12/tech/cnettechnews/main4443738.shtml

[16] J. Han, R. Kim, H. Youm, J. Ryou, "Survey of Traceback techniques and Requirements on Traceback in the NGN Environment", *JWIS2008*, pp. 267-281, July 2008.

## 〈著者紹介〉

**한 정 화 (Jung-hwa Han)**
학생회원

2007년 2월 : 순천향대학교 정보보호학과 졸업
2007년 3월~현재 : 순천향대학교 대학원 정보보호학과 재학(석사)
<관심분야> 네트워크 보안, 이동통신보안



**김 락 현 (Rach-hyun Kim)**
종신회원

1997년 2월 : 순천향대학교 전자공학과 졸업
1999년 8월 : 순천향대학교 대학원 전기·전자공학과 석사
2007년 2월 : 순천향대학교 대학원 정보보호학과 박사
2000년 2월~2007년 8월 : 순천향대 청운대학교, 홍성기능대학교, 아산정보기능대학 외래강사
2008년 3월 : 순천향대학교 정보보호학과 겸임교수
<관심분야> 암호 이론, 공개키 기반구조, 네트워크 보안, 보안 프로토콜, 이동통신보안

**류 재 철 (Jae-cheol Ryou)**
종신회원

1985년 2월 : 한양대학교 산업공학과 졸업
1988년 5월 : Iowa State University 전산학과 석사
1990년 12월 : Northwestern University 전산학과 박사
1991년~현재 : 충남대학교 정보통신공학부 교수
1993년~1995년 : JTC1/SC27 보안기술 전문위원회 위원
1995년~1996년 : 시스템공학연구소 초빙연구원
1997년~현재 : 한국정보보호학회 이사
2001년~현재 : 국가정보원 정보보호시스템 인증위원회 위원
2003년~현재 : 인터넷침해대응기술연구센터 센터장
<관심분야> 스마트카드 보안, 인증이론 및 시스템, 유·무선 인터넷 보안, 저작권 보호

**염 흥 열 (Heung-youl Youm)**
종신회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 2월 : 한양대학교 대학원 전자공학과 석사
1990년 2월 : 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, (현)상임부회장, (현)논문지 편집위원장
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2005년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2006년 11월~현재 : 정보통신연구진흥원 정보보호 전문위원
<관심분야> 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안