韓國 컴퓨터情報學會 2007하계학술발표논문집&학회지
第15卷 第1號, 2007. 6.

IP 역추적 설계 및 보안감사 자료생성에 관한 연구

이 인 희*, 박 대 우**

A Study regarding IP Traceback designs and security audit data generation.

In-Hee Lee*, Dea-Woo Park**

요 약

본 논문에서는 최근의 해킹사고에서 침입자는 피해시스템에서 자신의 IP주소 노출을 피하기 위하여 피해 시스템을 직접 공격하지 않고 Stepping stone(경유지)을 이용하여 우회 공격을 수행한다. 본 논문에서는 로그기반에서는 네트워크 감사 정책을 이용하고, TCP 기반에서는 CIS, AIAA 기법과 네트워크 기반에서는 Thumbprints Algorithm, Timing based Algorithm, TCP Sequence number를 이용한 알고리즘, Sleep Watermark Tracking 기법을 이용하여 역추적 시스템을 제시하였으며, 현 인터넷 망의 구성의 물리적 또는 논리적 복잡성이 크다는 단점을 보완하기 위해, 날로 발전하고 빠른 기술 개발 속도를 갖는 침입 기술에 대응하기위해 하나의 시스템에 하나의 모듈이 아닌 기존의 알고리즘을 이용해 효과적인 역추적 시스템을 제시 하려 한다.

Abstract

Avoid at damage systems in order to avoid own IP address exposure, and an invader does not attack directly a system in recent hacking accidents at these papers, and use Stepping stone and carry out a roundabout attack. Use network audit policy, and use a CIS, AIAA technique and algorithm, the Sleep Watermark Tracking technique that used Thumbprints Algorithm, Timing based Algorithm, TCP Sequence number at network bases, and presented a traceback system at TCP bases at log bases, and be at these papers Use the existing algorithm that is not one module in a system one harm for responding to invasion technology develop day by day in order to supplement the disadvantage where is physical logical complexity of configuration of present Internet network is large, and to have a fast technology development speed, and presentation will do an effective traceback system.

▸ Keyword : IP Traceback, Hacking, Forensics, Cyber Security.

• 제1저자 : 이인희, 교신저자 : 박대우(prof1@paran.com)
* 숭실대학교 정보과학대학원 정보보안학과, ** 호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

오늘날 컴퓨터 네트워크의 발전으로 많은 사람들이 인터넷의 혜택을 받고 있다. 전 세계에 연결된 글로벌 네트워크는 개인 홈페이지, 인트라넷 그리고 포털 서비스 등으로 확장되었고, 인터넷을 이용한 각종 사업이 이루어지고 있다. 이렇게 발전된 인터넷은 사용자들에게 많은 순기능을 제공하기도 하지만 인터넷의 개방으로 인한 보안의 취약성으로 개인과 기업 그리고, 국가의 기밀 정보가 유출되어 악용되기도 하며, 시스템에 치명적인 손상을 주는 일들이 증가하고 있다. 국내 통신망 인프라는 세계1위의 위치에 있을 정도로 잘 구축되어 있으나 보안에 대한 현실은 크래커들이 다른 나라의 Network를 침투하기 위한 경유지로 우리나라를 이용한다는 사실에서 잘 나타난다. 이러한 인터넷을 이용해서 실생활에서 수행해야만 했던 많은 일들을 인터넷을 통해 수행할 수 있게 되었고, 인터넷의 편리함 때문에 인터넷 사용자 역시 크게 증가하였다. 이러한 사용자의 증가와 더불어[그림 1]에서 볼 수 있듯이 인터넷을 통한 각종 침해사고 역시 크게 증가하였다[1].

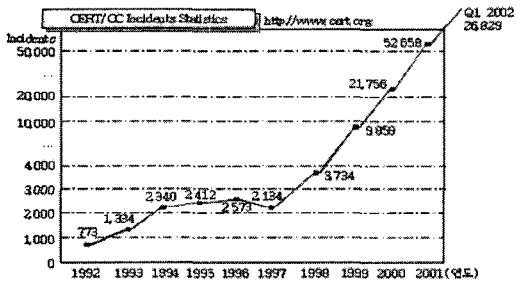

그림 1. 연도별 침해사고 횟수
Fig. 1. The infringement accident frequency by a year.

보안이라는 것은 보안에 대한 지식이 있을 때에만 보안의 중요성도 느끼게 되는 것이다. 보안에 대한 지식이 아니라 보안에 대한 관심만이라도 있으면 자신의 시스템에 허가 받지 않은 사용자의 침투 여부정도는 알 수 있을 것이다. 그렇지만 관심조차도 없다면 시스템의 불법 침투여부는 물론 보안의 중요성도 느끼지 못할 것이다.

따라서, 컴퓨터 네트워크에 대한 보호가 요구되어 방화벽이나 침입 탐지 시스템(Intrusion detection System), 침입 차단 시스템(Intrusion Prevention System), 통합 보안 시스템(Unified Threat Management) 등과 같은 침입 대응 시스템이 개발되어 광범위하게 사용되고 있다.

이러한 시스템들은 보안 침해 사고에 대한 사전 방지책이며, 보안 침해의 사후 처리에 대해 별다른 대응 방안을 제시해 주지 못하고 있다. 완전한 사전 방지가 보장되지 않는 상황에서는 사전 방지만큼이나 사후 처리도 보안 침해 사고 방지를 위해 중요한 조건이 된다.

컴퓨터 시스템으로의 침입은 알려지지 않은 사용자로부터 시작된다. 대부분의 보안 침해 사고들은 컴퓨터를 공격할 때 복잡한 경로(DoS)를 거쳐서 대상 컴퓨터에 접근하기 때문에 침입자의 처음 위치를 식별하기가 어렵다, 따라서 침입자를 효율적으로 추적하는 방안과 시스템에 감사 로깅 사용 내역을 기록하여 시스템의 안정성을 높이기 위한 도구들을 사용하여 시스템 내에서 수행된 각종 응용프로세스, 외부 통신망을 통해 접근하여 수행된 작업 내역 등의 정보를 기록하여 수집된 정보는 추후에 시스템 무결성을 확인하거나, 감사 정책의 효과적인 적용여부를 분석 자료로 제공하여 침입자를 추적하는 방안이 연구· 제시되어야 한다. 또, 침입자의 처음 위치를 알아냈다 하더라도, 그것이 위조된 경우가 아닌지 확실한 증거를 제시해야 하는 어려움을 가지고 있다.

본 논문에서서 보안침해 사고에 대응하기 위한 공격자의 역추적 방법을 제안하며 포렌식 자료를 통해서 침입자를 추적 할 수 있는 방안을 연구한다.

2장에서는 관련연구로 IP 환경에서의 역추적 기법으로 호스트기반 추적(Host-based Traceback), 네트워크 기반 추적(Network-based Traceback), 동적 네트워크 기반 추적(Active Network based Traceback)과 전향적 기법과 대응적 기법에 대해 알아보고, 3장에서는 TCP/IP 환경에서의 IP 역추적 기법 모델에 대해 설계한다. 4장에서는 TCP/IP 환경의 IP 역추적 기법 모델을 제시하고 효과적인 추적 모델을 연구하고 보안감사 자료를 생성한다. 마지막으로 5장에서는 결론을 내리고, 향후 연구에서는 유비쿼터스와 IPv6 무선 환경에서의 역추적 기법에 대해서 논의한다.

Ⅱ. 관련 연구

2.1. TCP 역추적 기법

역추적(Traceback)이란 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기술을 말하는 것으로 크게 2

가지로 분류할 수 있다. 본 장에서는 역추적 기술의 정의와 분류 그리고 현재 사용되고 있는 역추적 기법의 문제점에 대해 살펴보도록 한다.

TCP 연결 역추적 기술은 다시, 크게 2가지로 분류할 수 있다. 이는 호스트 기반 연결 역추적(host-based connection traceback) 기술과 네트워크 기반 연결 역추적(network-based connection traceback) 기술로 분류된다.

TCP 연결 역추적 기술은 흔히 연결체인 역추적 기술이라고 불리기도 한다. 여기서, 연결 체인이란 [그림 2]에서 H0에서 Hn까지의 연결들의 집합을 연결 체인[2]이라고 한다. 즉, 해커가 실제로 위치한 시스템으로부터 여러 시스템을 경유하여 실제 공격을 당하고 있는 시스템까지의 연결들의 집합을 말하는 것으로 다음과 같이 정의된다.

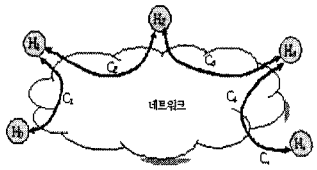

그림 2. 연결체인
Fig. 2.. A connection chain

2.2. Host 기반 역추적 기법

호스트 기반 연결 역추적 기술은 역추적을 위한 모듈이 인터넷 상의 호스트들에 설치되는 역추적 기법으로 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술이다. 그러나 이러한 방법을 이용하여 역추적을 수행하기 위해서는 인터넷 상의 모든 호스트에 역추적 모듈이 설치되어야 하고, 역추적 경로 상의 단 1개의 시스템에서라도 어떤 문제에 의해서 역추적 정보를 얻을 수 없게 되는 경우가 발생하면 역추적이 불가능하게 되는 단점을 가지고 있다[4,5,6].

2.3. 네트워크 기반 역추적 기법

네트워크 기반 연결 역추적 기술은 네트워크상에 송수신되는 패킷들로부터 역추적을 수행할 수 있는 정보를 추출하여 역추적을 수행하는 것으로 역추적 모듈이 네트워크상에 송수신되는 패킷을 확인할 수 있는 위치에 설치된다. 현재 제안되고 있는 방법은 대부분 송수신 패킷을 확인할 수 있는 위치에서 공격 연결과 같은 연결 체인에 속하는 연결을 추출하여 역추적을 수행하는 방법을 취하고 있다.

그러나 아직까지 네트워크 기반 연결 역추적 기술을 현재의 인터넷에 적용하여 사용할 수 있는 전체 시스템은 제안되지 못했다. 다만 네트워크상에서 얻을 수 있는 패킷으로부터 어떤 정보를 활용해야 공격 연결과 같은 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘만이 제기되고 있는 상황이다[3,7,8].

또 다른 네트워크 기반 연결 역추적 기술로는 액세스 네트워크상에서 동작하는 기술들이 있다. 그러나 액세스 네트워크를 기본으로 하기 때문에 현재의 인터넷 환경에 적용하는 데 많은 어려움이 있는 것이 사실이다[9,10].

2.4. IP 패킷 역추적 기법

IP 패킷 역추적 기술은 앞서 잠시 언급한 바와 같이 IP 주소가 변경된 패킷의 실제 송신지를 추적하기 위한 기술을 말한다.

일반적으로 IP 주소가 변경된 패킷은 악의적으로 사용되는 경우가 대부분이다. 특히 서비스 거부(Denial of Service: DoS), 혹은 분산 서비스 거부(Distributed Denial of Service: DDoS) 공격에 주로 사용된다. IP 주소가 변경되는 경우에는 TCP 연결을 유지할 수 없기 때문에, 일방적인 패킷 송신으로 공격이 가능한 DoS 혹은 DDoS에서 주로 사용되는 것이다. 물론 과거 IP spoofing이라 알려져 있는 해킹 기법을 이용하는 경우, IP 주소가 변경된 패킷을 이용하여 공격하고자 하는 대상 시스템에 백도어를 설치하도록 하는 기법이 사용되기도 하였으나, 이를 위해서는 TCP sequence number guessing 과정이 필요하기 때문에 최근에는 거의 사용되지 않고 있다. 또한 IP 패킷 역추적은 현재 특정 시스템으로 IP주소가 변경된 패킷을 송신하는 시스템을 찾는 기술로서, 여러 중간 경유지를 추적하여 실제 해커의 위치를 찾는 TCP 연결 역추적 기술과는 해결하고자 하는 문제의 대상에 약간의 차이가 있다.

IP 패킷 역추적 기법으로는, [그림 4]에서 볼 수 있듯이 해커가 전송하는 패킷에 해당 패킷을 전달한 라우터를 표시함으로써 추적할 수 있게 하는 패킷 표시 기법[11]을 이용한 연구와 다른 여러 기법을 통한 IP 패킷 역추적을 위한 연구[12]가 진행 중이다.

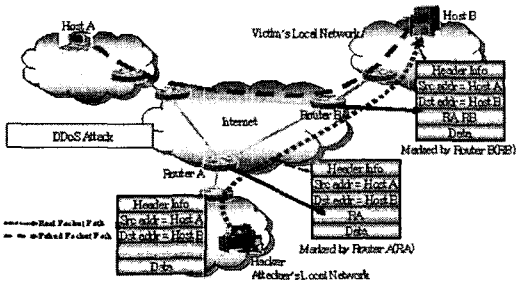

그림 3. IP 패킷 역추적
Fig. 3. IP packet Traceback

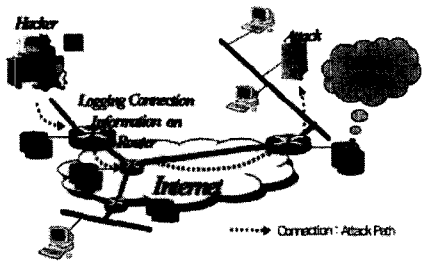

그림 4. 로깅기법 작동구조
Fig. 4. Logging Technique operation structure

2.4. 전향적 역추적 기법

2.2.1 링크 검사법

hop-to-hop 추적 방식에 해당하는 것으로 각 라우터에서는 연결된 링크에 대해 검사하면서 트래픽이 DoS 공격으로부터 전송된 패킷인지의 여부를 검사하게 된다. 자동화된 역추적 방법을 제공하지는 못하며 직접적으로 패킷 전송 경로를 조합/판별하는 방법에 해당한다. 따라서 네트워크 관리 측면에서의 오버헤드가 발생하게 된다. 링크 검사법에 대하 구현 결과로 제시된 input debugging 기법에서는 공격 유형(attack signature)을 기반으로 공격 트래픽에 대한 판별하고 실제로 전송된 경로를 판별한다. 그러나, 이 기법인 경우 서로 다른 ISP 관할 네트워크에 대한 검사에 한계가 있으며, 공격 유형에 대한 판별이 쉽지 않다. 링크 검사법의 또 다른 적용 기법으로는 controlled flooding 기법이 있다. 이 기법은 피해 시스템에서 상위 라우터로 패킷을 생성하여 전송하면서 반대로 DDoS 해킹 공격 패킷 량의 변화를 측정하고 최종적으로 공격 근원지를 찾아내는 방식이다. 그러나 이 기법 역시 DoS 공격의 일조에 해당할 수 있다는 단점이 있다.

2.2.2 로깅 기법(Logging)

로깅 기법[그림 4]은 라우터에서 전송된 패킷에 대한 특성 등을 기록해 놓은 후에 데이터 마이닝 등의 추론 시스템을 적용하여 공격 근원지를 검출하는 기법이다. 물론 많은 양의 정보를 저장/관리하고 있어야 하며 데이터 처리량 또한 방대하여 효율적인 대응 기법이라고 할 수는 없다.

이에 대한 해결책으로 확률적인 샘플링 기법 등을 적용하여 처리 데이터를 줄이고, 필터기법 등을 적용하여 처리/판별 과정을 간략화 하는 방법 등이 제시되기도 하였으나 방대한 패킷에 대한 판별 과정에서의 오류 수정 과정 등이 보완되어야 한다.

2.2.3 PPM 기법

스푸핑된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크상에 전송되는 패킷에 대해 네트워크를 구성하는 주요 요소인 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 헤더에서 변형 가능한 필드에 대해서 라우터에 해당하는 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다[그림 5].

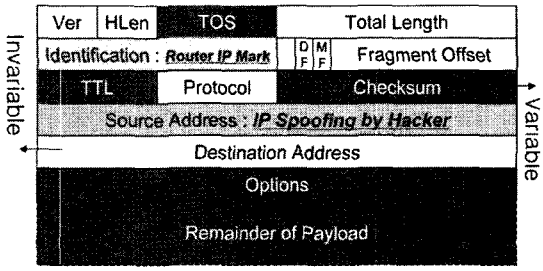

그림 5. 패킷 마킹을 위한 IP 헤더 구조
Fig. 5. IP header structure for packet marking

각 라우터에서 삽입된 정보는 다시 다음 라우터로 전달되고 최종적으로 목적지 피해 시스템에 전달된다. 각 라우터에서 마킹된 정보가 전달되면 추후에 해킹 공격이 발생하였을 경우 해킹 공격에 해당하는 패킷에 기록된 라우터 정보를 재구성(reconstruction)하여 실제적인 패킷의 전달 경로를 재구성하게 된다. 이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링(node sampling), 에지 샘플링(edge sampling) 및 개선된 패킷 마킹 기법 등이 제시되었다.

2.2.4 iTrace(ICMP Traceback)기법

ICMP 역추적 기법은 PPM 기법과는 다른 접근 방법으로 수행된다. 라우터에서는 일반적 $\frac{1}{20,000}$ 의 확률로 패킷을 샘플링 하여 iTrace 메시지를 생성하고 이를 패킷의 목적지 IP로 전송한다. iTrace 메시지는 일반적인 ICMP 메시지와 유사하게 전 단계 라우터 정보와 다음 단계 라우터 정보를 포함하고 있으며 패킷의 payload 정보 등을 포함 하여 전달하게 된다.

생성 시에 TTL(time of live) 필드 값은 255로 설정되어 전달되며 목적지에서는 TTL 값을 보고 네트워크 위상에서의 홉 거리 정보이기 때문에 공격경로 재구성에 사용된다. iTraceback 기법에 대한 작동방식은 [그림 6]과 같으나 일반적으로 PPM 기법과 마찬가지로 DDoS 공격에대응하기위해서는상대적으로많은정보가필요하기때문에개선된기법이제시되어야한다.

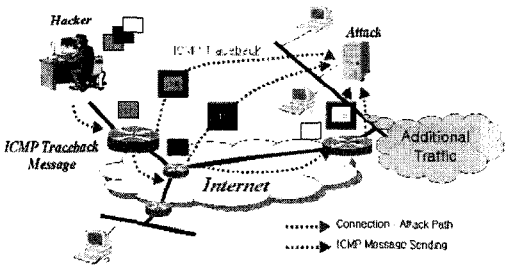

그림 6. iTrace 역추적 기법
Fig. 6. An iTrace Traceback technique

2.3 대응적 역추적 기법

2.3.1 오버레이 네트워크 역추적 기법

본 기법은 역추적 라우터(TR : tracking router) 모듈을 네트워크에 별도로 설치하고 해킹공격이 발생하였을 경우, [그림 7]네트워크위상에서의 종단시스템과 연결된 라우터에서 전달된 정보를 TR로 전송한다. 즉, 기존의 ingress 필터링 기법과 유사하게 종단 라우터에서 보내진 트래픽정보는 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 전체네트워크를 관리할 수 없기 때문에 소단위 네트워크에 적합한 기법이다. 또한 단일 ISP 네트워크상에서 구현 가능한 기법이며 이 기종의 네트워크 환경에는 적용할 수 없다. 또한 해킹공격은 짧은 기간 동안에 수행될 수 도 있기 때문에 전체경로를 역추적 하는데 어려움이 발생할 수 도 있으며, 공격자에 의해서 터널링된 패킷이 위조될 수 도 있기 때문에 보안상의 문제가 발생하게 된다.

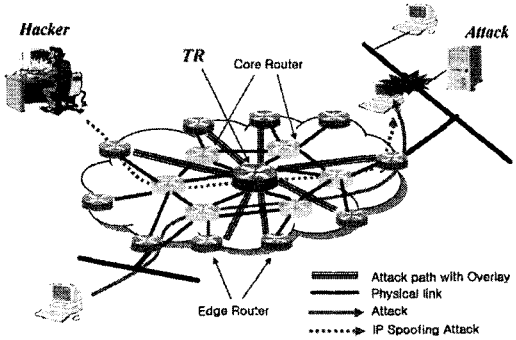

그림 7. 오버레이 네트워크 기반 역추적
Fig. 7. Overlay Traceback based a network

2.3.2 해쉬기반 역추적 기법

본 기법은 SPIE(source path isolation engine) 기반 역추적 서버를 구성하고 전체네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리한다. 그리고 각 라우터에는 DGA(data generation agent) 기능을 탑재하여 운영한다.

DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬값에 해당하는 IP헤더 정보와 8 바이트정보의 payload 정보를 수집관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 목적지 시스템에 있는 IDS 시스템에 의해 해킹을 발견하였을 경우 SPIE 시스템에서는 네트워크 그룹을 관리하는 SCAR 에이전트를 통해 그룹 내 DGA 라우터에 저장된 정보와 해킹 패킷정보를 비교 분석하여 이를 다시 SPIE 시스템에 전달하게 되면 해킹 관련 패킷의 전송경로를 재구성하게 된다.

본 기법을 적용하기 위해서는 [그림 8]SPIE, SCAR 및 DGA 기능을 구축하여야하며 추가적인 모듈로 제공되기 때문에 이 기종 환경의 ISP간적용도가능하다. 실험결과 0.5% 정도의 추가적인 해쉬 정보가 생성되어 전달되고 SCAR에서는 주기적으로 패킷에 대한 해쉬값을 관리하기 위한 메모리가 필요하다.

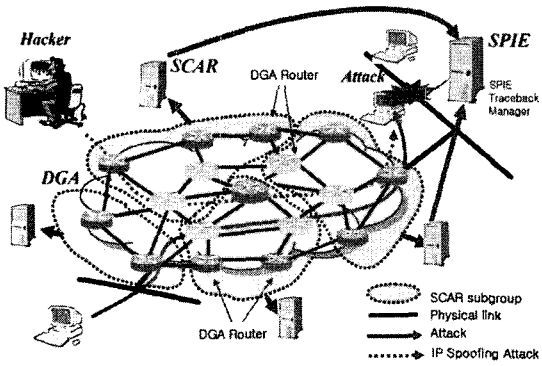

그림 8. 해쉬기반 역추적 기법
Fig. 8. A Hash based Traceback technique

2.3.3 IPSec 기반 역추적 기법

본 기법은 오버레이 네트워크 기반 역추적 기법에서 발생하는 터널링 과정에서의 보안상 취약점을 보완하기 위해 제시된 기법이다. 전체 네트워크에 대한 위상을 각 라우터가 알고 있다는 가정 하에 해킹공격이 발생하게 되면 네트워크상의 라우터와 피해 시스템 간에 IPSec 연결이 구성되어 공격자에 의한 공격패킷이 해당 라우터를 통해 전송 될 경우 IPSec 터널을 통해 경로 정보를 피해 시스템에 전달하게 된다. 다시 네트워크 위상에서의 주변라우터를 선정하여 IPSec 터널을 구성하고 패킷에 대한 전송여부를 판별하여 이를 피해 시스템에 전달하는 과정을 반복한다[그림 9].

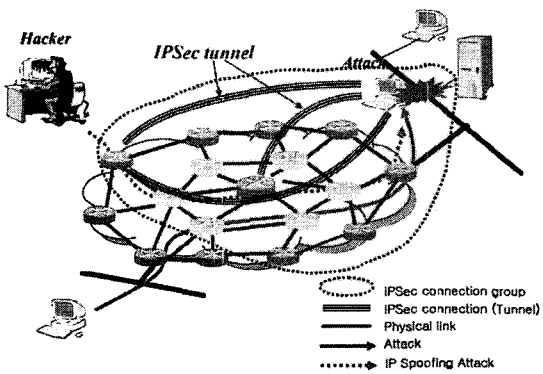

그림 9. IPSec 기반 역추적 기법
Fig. 9. A Traceback technique-based IPSec

이와 같은 과정을 통해 해킹 공격 발생 시 실제적으로 패킷이 전송된 경로상의 라우터를 판별할 수 있게 된다. 물론 IPSec을 이용한 역추적 방식은 피해시스템과 라우터 간에 IPSec 터널연결을 구성한 경우에는 공격 경로를 파악할 수 있으나, IPSec 연결을 취하지 않는 네트워크에서는 경로 재구성에 어려움이 있게 된다. 아래 [표1]는 대응적 IP 역추적 기법과의 성능 비교 평가를 보여주고 있다.

[표 1] 대응적 IP 역추적 기법과의 성능 비교 평가
Fig. 1. Evaluation comparative performance with a Reactive IP Traceback technique

특성 / 기법	네트워크 부하	피해 시스템 부하	메모리 요구	역추적 기능	보안기능	DDoS 대응
Overlay Network	↓	↓	↓	△	◇	◇
Hash based TB	↓	↓	↓	△	△	◇
IPSec based TB	↓	↑	×	△	△	▽

×:N/AT ↑:high, ↔:middle ↓:low △:good ◇:moderate ▽:bad

III. IP 역추적 모델 설계

TCP/IP의 감사 기록을 이용한 IP 역추적 설계 및 포렌식 의 생성을 위해 로그기반 침입자 역추적 기법과 TCP 기반 연결 역추적 설계와 네트워크 기반 연결 역추적 알고리즘을 사용한다.

3.1. 로그기반 침입자 역추적 설계

네트워크의 감사 기록 추적은 네트워크에서 외부 사용자에 의해 요청되는 각종 서비스 기능이 수행될 때 공격자의 분석 및 저해 요인에 대한 제어 절차 개발과 설정된 보호 정책을 허용하며 시스템 제어에서 부 적절성을 지적할 수 있는 정보를 보고하고 제어, 정책, 절차상에서 요구된 변경 사항을 저장하도록 해야 한다. 네트워크 보호와 관련된 사건은 감사의 대상 자료가 될 수 있는데 감사 자료의 종류는 크게 두 가지로 분류 된다.

- 네트워크 보안에 관련된 감사 자료
  - 시스템과 시스템들 사이의 접속.
  - 시스템에 요청된 서비스 종류(Ftp, Rlogin, Telnet,..... 등).
  - 네트워크에서의 Traffic 양.
- 시스템 보안에 관련된 감사 자료
  - 시스템 자원에 관련된 감사 자료(CPU 사용량, I/O 장치 사용량등).
  - 사용자 로그인 실패 횟수.

- 사용자 패스워드 실패 횟수.
- 파일 시스템에 관련된 감사 자료(Read, Write, delete, Create, Append등).
- 시스템 파일에 관련된 감사 자료.
- 한 세션 안의 사용자의 지속 시간.
- 한 세션 안의 사용자의 출력 데이터의 종류 및 양.

이러한 감사 자료를 바탕으로 감사 추적 기법을 이용, 사용자의 행동 패턴을 통하여 시스템 사용에 대한 감사 추적을 수행 할 수 있다.

별도의 역추적 설비가 없는 시스템에서는 UNIX의 기본적인 로그 정보를 바탕으로 특정 사용자나 호스트의 정체를 파악하기 위해 관련 명령어를 사용하여 침입자를 추적할 수 있다[9].

불법 침입자의 침입흔적은 시스템의 각종 로그 파일에 남는다. 시스템에 대한 스캔 행위, exploit 툴을 이용한 공격, 특정 사용자 계정으로의 접속, root 권한의 획득, 트로이목마 프로그램 설치, 자료 유출 및 삭제 등 공격자의 행위 하나 하나가 모두 시스템에 의해 감시되고 로그로 남게 된다. 일반적으로 사용자 추적에 사용되는 명령어는 finger, users, whodo 등이 있다. 또한 현재 사용자가 시스템에서 활동 중일 경우, 사용자의 연결 상태와 활동을 파악하기 위해 netstat 명령어를 사용한다. 사용자 추적에 사용될 수 있는 로그 파일들로는 utmp, wtmp, acct, lastlog, messages 등의 로그 파일들이 있으며, 이러한 로그 파일들은 자동으로 생성된다. 리눅스를 포함한 유닉스 시스템은 로그의 종류 및 로그의 위치가 시스템마다 조금씩 차이가 있다.

그러나, 이러한 명령어와 로그 파일의 정보를 이용하여 컴퓨터 네트워크 침입자를 역추적 하는 방법은 여러 가지 한계가 있다. 첫째, 관리자가 방대한 로그 파일을 이용하여 직접 수작업을 해야만 한다. 따라서, 침입자가 자신의 자취를 은폐할 수 있는 충분한 시간을 얻을 수 있다. 둘째, 로그 파일이 제공하는 많은 정보 중에서 침입자의 추적에 관계되는 확실한 증거를 찾아내기 어렵다. 셋째, 로그 파일의 정보는 침입자가 쉽게 위조할 수 있기 때문에 로그 정보를 이용하는 방법은 신뢰성을 보장받지 못한다.

3.2. TCP 기반 연결 역추적 설계

3.2.1 CIS[4]

H.T. Jung에 의해 1993년 제안된 CIS(Caller Identification System)시스템을 이용하여 IP 역추적을 설계한다[그림 10]. CIS는 사용자가 특정 시스템에 접속하고자 할 때, 해당 시스템은 접속을 시도하는 사용자가 그 이전에 거쳐 왔던 모든 시스템에 대한 시스템 목록과 로그인 ID 등의 정보를 요구한다. 그리고 요구에 따라 이전의 경유 시스템 목록을 입력 받게 되면, 모든 경유 시스템과의 통신을 통해 각 시스템에 대해 입력된 시스템 및 로그인 ID 목록이 정당한 것인지를 확인하게 되고, 이러한 목록이 유효할 때만 접속을 허락한다. 이런 형태의 역추적 시스템은 미리 사용자가 지나온 시스템의 목록을 관리하는 것이다.

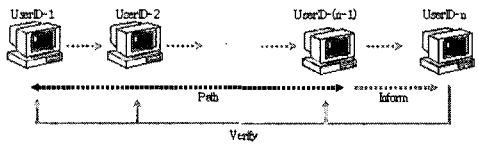

그림 10. CIS 구성도
Fig. 10. A CIS formation table

3.2.2 AIAA[5]

AIAA(Autonomous Intrusion Analysis Agent) 시스템은 침해를 당한 서버의 해킹 피해 분석과 추적을 위한 로그 분석 에이전트를 이용해 자동화한 역추적 시스템이다. AIAA 시스템은 침입자가 거쳐 온 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.

[그림 11]의 시스템은 역추적 경로 상에 존재하는 시스템들의 관리자의 도움을 받아 설치하기 때문에 역추적을 완료하기까지 많은 시간이 필요하게 된다. 또한 역추적 경로 상에 존재하는 모든 시스템에 직접 접속해야 하기 때문에 만약 관리자와의 협조가 불가능하여 시스템으로의 접근이 불가능한 경우 역추적 자체가 불가능할 수도 있다.

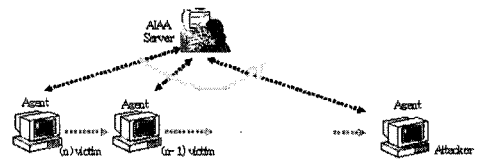

그림 11. AIAA 침입분석 구성도
Fig. 11. An AIAA invasion analysis formation table

3.3 네트워크 기반 연결 역추적 설계

3.3.1 지문 알고리즘의 설계

지문 알고리즘을 이용하는 방법은 역추적 시스템 전체를 의미하는 것이 아니라 역추적을 위해 공격자의 시스템으로부터 공격 대상 시스템까지의 연결 체인을 구성하는 알고리즘이다. 본 알고리즘은 연결 체인에 속하는 호스트들이 속한 네트워크상에 송수신되는 데이터를 수집하여 비교한다.

[그림 12]을 이용한 방법의 아이디어는 공격자의 시스템으로부터 해커가 위치하고 있는 시스템까지의 연결 체인에 송수신되는 데이터는 동일할 것이라는 점을 이용한다. 즉, 공격에 사용되는 연결에서 송수신 되는 데이터로부터 추출한 내용 정보를 특정 함수를 적용하여 얻어낸 지문이 일정수준 이상 동일한 경우 두 연결은 하나의 연결 체인상에 존재하는 것으로 판단한다.

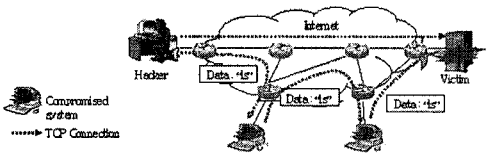

그림 12. 지문기반 알고리즘
Fig. 12.. Thumbprints base algorithm

3.3.2 타이밍 기반 알고리즘의 응용

타이밍기반 알고리즘을 이용한 방법 역시 연결 체인을 구성하기 위한 알고리즘이다. 본 알고리즘은 해커가 입력하는 키보드 입력에 의해 발생하는 데이터 송신 간격은 프로그램이 송신하는 데이터에 비해 매우 크기 때문에, 이를 쉽게 파악할 수 있고, 만약 같은 연결 체인에 속한다면 그 간격이 매우 유사할 것이라는 점을 이용한다. 이 시스템은 ON period와 OFF period를 이용하여 각각의 상태가 변화하는 시점과 한 상태를 유지하는 시간 간격을 분석하여 같은 연결 체인에 속하는지 여부를 판단하게 된다.

3.3.3 TCP sequence number를 이용한 알고리즘의 응용

TCP sequence number를 이용하는 알고리즘은 비록 송수신되는 데이터가 암호화 되더라도 데이터의 양은 크게 변하지 않는다는 점에 착안하여 sequence number의 증가 정도를 변동 폭의 조정을 통해 비교하고 연결 체인을 구성하는 알고리즘이다[그림 13].

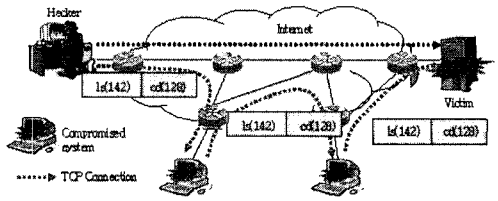

그림 13. TCP Sequence Number를 이용한 알고리즘
Fig. 13. The algorithm that used TCP Sequence Number

3.3.4 SWT(Sleepy Watermark Tracing)의 응용

SWT 역추적 시스템은 침입에 대한 응답 패킷에 워터마크를 삽입하여 역추적을 수행한다. SWT 기법은 한 네트워크에는 guardian gateway와 연동되어 동작하는 guarded host가 존재한다고 가정한다. 침입이 발생되면 guarded host내의 IDS에 의해 탐지되고 guarded host의 SWT subsystem의 sleepy intrusion response 모듈의 작동이 시작된다. 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.

IV. IP 역추적 실시 후 보안감사 자료 생성

4.1. 로그기반 IP 역추적

VoIP 서비스에 대한 스팸 공격을 차단할 수 있는 방법들을 제안한다. 제안된 방법들에 대한 시험실에서의 시험을 통해 스팸 차단이 되는 지의 결과를 시험한다.

네트워크상에서는 사용자의 로그인, 로그아웃 정보와 명령어 실행 정보, 다양한 응용 프로그램을 수행한다. .cshrc, .profile등에 미리 규정된 응용 프로그램을 기본 수행하는 것은 물론, shell 인터페이스를 통해 응용 프로

그램의 수행을 지시하거나, 한 응용 프로그램 내부에서 fork, exec 등을 통해 다른 응용 프로그램을 구동 시킬 수 있다. 원칙적으로 응용 프로그램의 수행 없이 시스템 자원에 대한 접근이 이루어 질 수 없으므로 사용자별 응용 프로그램 수행 내역은 감사 로깅 시스템에서 네트워크에 대한 불법 접근을 추적할 수 있는 매우 유용한 정보가 된다. 따라서 본 논문에서는 운영체제의 커널로부터 프로세스 정보를 직접 입수해야 하는게 더 효과적이다. 침투 단계에 나누어 3단계로 설명할 수 있는데 각 단계의 침투 유형을 볼 수 있다.

〔표 2〕 침투 단계에 따른 대응방법
Fig. 2. A response way along a penetration step

단계	침투방법	대응방법
1단계	일반 사용자의 ID 및 패스워드 도용한 일반 사용자 로그인	제한하지 않음
	시스템 관리자인 ID 및 패스워드를 도용한 시스템 관리자 로그인	보안 쉘 프로그램에서 검사하여 연결 해지시킨다.
	시스템 콘솔을 이용한 시스템 관리자 로그인	제한하지 않음
2단계	일반 사용자의 시스템 관리자 권한 획득	프로세스의 UID와 TTY를 검사하여 UID가 0이고 TTY가 콘솔이 아니면 연결 해지시킨다.
	시스템 관리자의 시스템 내부 침투 공격	로그 파일로 기록을 남긴다.
3단계	감사 로깅 프로세스의 동작을 정지시키려는 시도	감사 로깅 프로세스의 ID를 계속해서 바꿈으로서 프로세스에 대한 공격 방어
	감사 로그 파일을 삭제하려는 시도	하드 링크를 연결하여 파일을 보호하고 외부 프로세스를 모두 종료 시킨다.
	감사 로그 파일을 변조하려는 시도	파일의 상태 정보에 이상이 발견되면 외부 프로세스를 모두 종료시킨다.

〔표 2〕은 네트워크상에서의 단계별로 침투하는 모습을 보여주고 있는데 1단계에서는 누구나 일반 사용자 ID를 이용한 로그인은 허락하고 있다. 콘솔이 아닌 곳에서 슈퍼유저 ID를 사용하여 로그인 감사 로깅 시스템에서는 먼저 슈퍼유저로 시스템에 접근하려는 것을 제한하고 슈퍼유저는 콘솔에서만 접근할 수 있도록 하고 2단계에서는 일반 사용자가 슈퍼유저로 권한을 얻는 경우 일반적으로 su 명령어나 setuid 프로그램을 이용하여 슈퍼유저 권한을 얻으려 할 것이다, 이러한 경우 로깅 프로세서에서는 로그 프로세스 정보를 커널에서 가져올 때마다 UID와 TTY를 검사하여 콘솔이 아닌 곳에서 일반 사용자가 슈퍼유저의 쉘 권한을 획득하는 것을 감시한다. 내부 사용자는 모든 내역이 로깅 프로세스가 기록하여 활동을 감시한다. 3단계에서는 침입자는 자신의 활동이 기록되는 것을 감추기 위해 감사 로깅 프로세서의 작동을 중지하려고 시도 하거나 프로세스를 종료시키고 로그 파일을 변경 또는 삭제 하려 할 것이다. 이러한 공격에 대응하여 슈퍼유저 권한을 갖는 사용자라도 감사 로그 파일을 강제로 삭제 할 수 없도록 해야 한다. 또한 감사 로그 파일을 변조하려는 경우에는 로그 파일을 수정 할 수 없도록 로그 파일에 강제적으로 파일 잠금을 해야 한다.

4.2. TCP 기반의 DoS, DDoS 공격에 대한 IP 역추적

인터넷에서 발생 가능한 해킹 공격에 대한 대응방안으로 현재까지 제시된 기법을 고찰해보면 네트워크를 통해 지속적으로 이상적 작동방식을 보이는 흐름에 대한 대응방식 이라고 할 수 있다. TCP SYN 공격이나 ICMP ECHO 패킷 등에 대한 공격을 살펴보면 많은 양의 트래픽이 네트워크를 통해 전달되고 또한 특정 목적지로 트래픽이 전달되는 특성을 보이고 있다. 따라서 인터넷에서 발생하는 해킹 공격은 네트워크를 구성하는 라우터에서 고찰하였을 경우 일종의 폭주(congestion) 현상으로 파악 할 수 있다. 결국 해킹 공격에 대한 대응 방안으로는 종단 간 폭주 제어 및 대응 기술로 접근 할 수 있다. DDoS 공격인 경우 하나 이상의 호스트로부터 네트워크상의 목적지 호스트로 많은 양의 트래픽이 전달되는 형태이기 때문에 인터넷에서의 해킹 공격에 대응하기 위해서는 DDoS 트래픽 특성을 파악하고 이를 차단하는 방식을 적용할 필요가 있다.

라우터에서의 DDoS 트래픽 제어 기술로 제시 된 것이 ACC(*aggregate-based congestion control*) 및 *pushback* 기술을 사용하는데, 이 기술은 라우터에서 주기적으로 네트워크 트래픽에 대한 모니터링 과정을 수행 하면서 만일 해킹 공격과 유사한 형태의 트래픽이 발생 할 경우 이를 판별한다. 라우팅 테이블에서 blue/yellow/orange/red로 분류하여 라우터의 부하를 줄이면서 동일한 라우팅 정책으로 하나의 관리자에 의하여 운영되는 네트워크, 즉 한 회사나 단체에서 관리하는 라우터 집단을 자율 시스템(AS, Autonomous System)이라 하며 각각의 자율 시스템을 식별하기 위한 인터넷 상의 고유한 숫자를 망식별 번호(AS 번호)를 이용한다. AS번호는 2바이트(0 ~ 65535)로 구

성되어 있으며 64512 ~ 65534까지는 사설 AS번호로 내부 네트워크에서 BGP(Border Gateway Protocol)를 적용할 때 사용되고 AS번호의 도입은 인터넷의 확산으로 네트워크의 크기가 커지고 라우팅 정보가 방대해지자, 전체 네트워크를 하나의 라우팅 프로토콜로 관리하는 것이 불가능해졌고. 이에 따라 네트워크의 관리범위를 계층적으로 체계화하고 단위 별로 라우팅 정보를 효율적으로 관리하기 위하여 AS(자율 시스템, Autonomous System)가 도입하였다[그림 14]. 그래서 AS가 도입되면서 라우터는 인터넷에 있는 모든 네트워크의 도달가능정보를 가질 필요 없이 자신의 AS 내에 있는 라우터에 대한 도달가능정보만을 가지면 된다.

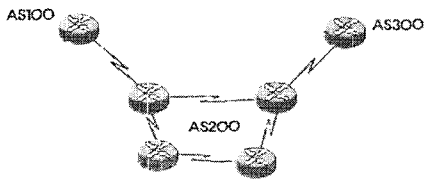

그림 14. AS망을 이용한 네트워크 구성도
Fig. 14. The network formation table which used an AS network

AS번호가 도입되면서 상위 ISP, IX와 연결된 다중 연결 사이트를 구성하는 경우 필요하며 다중 연결 사이트에서의 도달가능 정보를 여러 ISP에 배포하므로 라우팅 정책에 혼란을 막아주며 AS간의 질의 과정을 통해 라우터에서 보내오는 정보에 대해 검증하게 되고 결과적으로 라우터 정보를 신뢰할 수 있는 구조를 제공하게 된다. 이와 같은 구조는 라우터에서 인접 AS에 대해 검증 정보를 관리하고 인증 과정을 수행하면서 결과적으로 라우팅 테이블에 저장되어 있는 정보를 신뢰하게 된다. 검증 절차를 사용함으로서 AS가 자신의 라우팅 정책과 도달 가능성 정보를 책임 있게 배포 할 수 있다. 그러므로 AS 번호는 인터넷 상에서의 독립적인 네트워크를 식별 할 수 있어서 네트워크에 부하를 줄이고, 외부 네트워크와의 단일 경로를 교환하므로 신뢰성을 가질 수 있으며, 고유한 라우팅 정책을 구현하여 관리의 효율성을 가질 수 있다.

4.3 네트워크 기반 공격의 Honeypot에서 IP 역추적

침입 유도 시스템은 침입자가 발견되었을 때, 이 침입자가 시스템의 중요한 자료가 있는 곳으로 접근할 수 없도록 하거나 공격 형태의 분석 및 역추적을 위해 침입자를 유인하는 가상의 서버 시스템이다. 침입 유도 시스템에는 허니팟 시스템(Honeypot System), 피쉬볼 시스템(Fishbowl System)이 있다. 허니팟 시스템은 침입자를 유인하기 위한 가상의 시스템이다. 일반적으로 침입자가 취약점을 가진 컴퓨터를 골라서 공격한다는 점을 이용한다. 흔히 침입자는 자신이 공격할 컴퓨터를 선택하기 위해 많은 수의 컴퓨터를 조사하게 된다. 이 과정에서 허니팟은 침입자의 출현을 감지하여 의도적으로 만든 취약점을 드러내 침입자를 유인한다. 침입자가 출현하면 허니팟 시스템이 작동하여 침입자를 유인하며, 유인된 침입자의 움직임을 주시하면서 해킹의 신기술을 지켜볼 수 있고, 신분확보도 가능하다.

4.4 콘텐츠 필터링의 IP 역추적

콘텐츠 필터링은 이메일 스팸 차단 방법 중 가장 널리 적용된 방법이다. 콘텐츠 필터링은 수신된 이메일의 내용을 검사하고 분석해 스팸으로 의심되는 메일들을 제거하는 것으로 본 논문에서는 베이지안(Bayesian) 필터링[13] 방법을 사용하려고 한다.

베이지안식 접근이란 텍스트 분류(Text Classification)에 적용한 것으로 특정 텍스트에서 해커들이 사용하는 특정 개별 단어의 출현 빈도를 모두 기록한 뒤, 비슷한 분류의 텍스트를 계속 샘플 데이터로 추가 시켜나가면서 단어들의 연관을 추적하여 임의의 텍스트가 해당 분류에 속하는지 여부를 알 수 있다는 이론이다. 이 이론이 패킷 필터링을 충분히 포함하는 데이터들을 검사하는 방법으로 사용되어 질 수 있다. 베이지안 필터 학습을 통한 이러한 접근은 해커가 무의식적으로 사용하는 또는 사용할 수밖에 없는 어휘들을 인지할 수 있어 특히 효과적이다.

베이지안 필터의 주요 특징 중 하나는 분류하고자 하는 대상, 즉 IP의 Payload[그림 15]의 데이터에 대하여 '미리 정의된 규칙' 같은 것이 존재하지 않는다는 것이다.

모든 규칙은 자기 스스로 만들어내고, 자기 필터링 존에 들어와 학습된 데이터에 대해서 분석 꼬리표를 달아놓으면 그 순간 규칙이 작동한다. 보다 많은 확실한 스팸 샘플을 가지고 있을수록, 그리고 필터를 오래 사용할수록 필터는 더 정교하고 똑똑해진다. 이른 바 학습(training)에 의해 개인에 특화된 규칙들을 스스로 만들어나가는 응용기술이다.

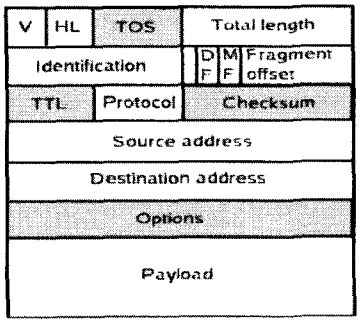

그림 15. IP Packet 헤더 형태
Fig. 15. An IP Packet header form

4.5 보안감사 자료의 생성

본 논문에서 제시한 로그인 세션동안 다양한 응용 프로세스를 실행할 때 응용 프로그램의 수행 내역에 대해서 운영체제의 커널로부터 직접 로그 정책을 관리하고, 네트워크상의 사용자의 로그인, 로그아웃 정보와 명령어 실행 정보를 3단계로 나누어 관리하고 기록함으로서 침입자에 대한 역추적을 효율적으로 관리 할 수 있고, 네트워크 에서는 주변 라우터에 대한 검증 구조를 제공해서 BGP 라우터에 의해 전체적인 라우팅 정보를 항상 정확하게 관리할 수 있으면 네트워크를 해킹 공격으로부터 안전하게 보호할 수 있다.

결국 기존의 라우터에 대한 보안 기능을 강화하게 되어 전체적인 라우터 구조에서의 신뢰성을 높을 수 있으며, 안전성이 향상된 라우팅 환경을 기초로 패킷에 대한 역추적 정보 등을 제공한다면 보안 기능이 강화된 라우터를 근간으로 DDoS 해킹이 발생하였을 경우 이에 대한 역추적 근원지를 신뢰 할 수 있다. 또한 보안 강화된 AS 망을 통과하는 모든 응답 패킷에 워터마크를 삽입하여 네트워크를 통해 들어온 패킷의 경로를 재구성 하는 알고리즘을 적용하여 신뢰성 있는 연결 체인을 구성하고 IP의 Payload 패킷을 분석하여 blue/yellow/orange/red 경고 시스템을 구성하고 패킷을 단계별로 구분하여 네트워크의 부하를 줄일 수 있으며, 해커가 입력하여 발생하는 데이터 발생 빈도 및 특정 데이터를 조사하여 패킷 필터링의 학습 효과를 이용한 정교한 규칙들을 만들어 간다면 신뢰성 있는 역추적 시스템으로서 차후에 침해 사고가 발생하였을 경우 각각의 단계에서 얻어진 데이터를 보안감사 자료를 생성하여 좀 더 빠르게 사고에 대응 할 수 있는데 효과적이다.

V. 결론

본 논문에서는 현재까지 연구되어온 역추적 기술을 분석한 결과 현재의 인터넷 망에 적용하기에는 문제점들이 많이 있었다, 인터넷 망의 구성이 물리적 또는 논리적으로 복잡성이 크게 있다는데 있다, 그리고 시간이 지남에 따라 침입 기술은 지능화 되고 해킹 또는 침해 유형에 대한 보안 강화 도구의 기술 개발 속도가 느리다는 점이고 또 하나의 이유는 하나의 시스템 또는 하나의 모듈을 이용해 모든 침입에 대한 역추적을 수행하려 하기 때문이다. 본 논문에서 제안하는 방법은 1차 서버에서는 혼잡 시그너쳐를 기준으로 필터링 모듈을 접목하여 네트워크의 패킷을 blue/yellow/orange/red 로 분류하여 red로 분류되어 의심되는 패킷은 허니팟 시스템이 작동하여 침입자를 유인하며, 유인된 침입자의 움직임을 주시하면서 해킹의 신기술을 지켜볼 수 있고, 신분확보도 가능하며, 역으로 추적을 시행하고, 서버의 부하를 줄여주는데 목적이 있다, 2차 서버로 넘어온 패킷에 대해서 IP의 Payload의 데이터를 콘텐츠 필터링하여 의심되는 데이터에 꼬리표를 달아두어 표시를 함으로서 학습에 의해 점차 정교하게 필터링 처리가 되는 과정을 만들어 가며, 3차 서버에서는 로그 기반의 감사 정책을 수립하고 데이터의 무결성을 확립하여 차후에 보안감사 자료로서 데이터의 신뢰성을 갖게 하는데 목적이 있다[14].

향후 연구에서는 무선 환경에서의 유비쿼터스와 IPv6 환경에서의 역추적 기법에 대해서 논의한다.

참고문헌

[1] http://www.cert.org

[2] Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, "Packet Tracker Final Report," CERIAS Technical Report 2000-23, Purdue University, 2000.

[3] K. Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders," In F. Guppens, Y. Deswarte, D. Gollamann, and M. Waidner, editors, 6th European Symposisum on Research in Computer Security - ESORICS 2000 LNCS -1985, Toulouse, France, Oct. 2000.

[4] H.T. Jung et al. "Caller Identification System in the Internet Environment.,"Proceedings of the 4th Usenix Security Symposium, 1993.
[5] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent," FIRST Conference on Computer Security Incident Handling & Response 1999.
[6] Steven R. Snapp, James Brentano, Gihan V. Dias, "DIDS(Distributed

[7] S. Staniford-Chen and L.T. Heberlein. "Holding Intruders Accountable on the Internet,"In Proceedings of the 1995 IEEE Symposium on Security and Privacy, 1995.
[8] Y. Zhang and V. Paxson, "Detecting Stepping Stones,"Proceedings of 9th USENIX Security Symposium, Aug. 2000.
[9] D. Schnackenberg, K. Djahandari, and D. Sterene, "Infrastructure for Intrusion Detection and Response,"Proceedings of DISCEX, Jan. 2000.
[10] D. Schnackenberg, K. Djahandary, and D Strene, "Cooperative Intrusion Traceback and Response Architecture(CITRA),"Proceedings of the 2nd DARPA Information Survivability Conference and Exposition(DISCEXII), June 2001.
[11] Dawn X. Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback,"Proceedings of InfoCom 2001.
[12] Stefan Savage, David Wetherall, Anna Karlin "Practical Network Support for IP Traceback,"Proceedings of the 2000 ACM SIGCOMM Conference, Stockholm, Sweden, Aug. 2000, pp295-306.
[13] 김현준, 정재은, 조근식. "가중치가 부여된 베이지안 분류자를 이용한 스팸 메일 필터링 시스템" 한국정보과학회논문지, 제31권8호, pp1092-1100, 2004
[14] 박대우, 임승린. "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구." 한국컴퓨터정보학회논문지, 제11권 제2호, pp44-50, 2006. 5. 31.

저 자 소 개

이 인 희

2000년 한신대학교 컴퓨터학과 졸업 (학사)
2005년 숭실대학교 정보과학대학원 정보보안학과 (석사과정)
2006년 숭실대학교 정보과학대학원 정보보안학과 조교
2007년 대한주택공사 R&D 연구원
〈관심분야〉 역추적기법, 포렌식, 인터넷 보안, 정보보호

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬 정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality