IP 역추적 기술을 이용한 능동형 보안 시스템

김재동* · 채철주* · 이재광*

Active Security System using IP Traceback Technology

Jae-Dong Kim* · Cheol-Joo Chae* · Jae-Kwang Lee*

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음
(IITA-2006-C1090-0603-0027)

요 약

최근 기술의 발전으로 인해 인터넷이 정보화 사회의 기반이 되는 기술로 발전하고 있는 반면 역기능인 해킹, 바이러스, 정보변조 등과 같은 기술 또한 발전하고 있다. 이러한 역기능에 대응하기 위해 방화벽(Firewall), 침입탐지 시스템(Intrusion Detection System) 등과 같은 보안 시스템이 개발되었지만 해킹 사고는 꾸준히 증가하고 있다. 기존의 이러한 수동적인 보안 시스템은 능동적인 시스템으로 발전되었다. 이에 본 논문에서는 IP 역추적 기술을 이용한 능동적 보안 시스템을 제안한다. IP 역추적을 위해 ICMP 형태의 역추적 메시지를 구현하고 지역 네트워크에 배치되는 에이전트와 관리 네트워크에 배치되는 서버 프레임워크를 설계하고, 이러한 능동형 보안 시스템을 기반으로 네트워크 기반의 침입자를 추적하고 고립화하기 위한 보안 메커니즘을 구현한다.

ABSTRACT

There is a tremendous increase in the growth of Internet making people's life easy. The rapid growth in technology has caused misuse of the Internet like cyber Crime. There are several vulnerabilities in current firewall and Intrusion Detection Systems (IDS) of the Network Computing resources. Automatic real time station chase techniques can track the internet invader and reduce the probability of hacking Due to the recent trends the station chase technique has become inevitable. In this paper, we design and implement Active Security system using ICMP Traceback message. In this design no need to modify the router structure and we can deploy this technique in larger network. Our Implementation shows that ICMP Traceback system is safe to deploy and protect data in Internet from hackers and others.

키워드

능동 보안 시스템, IP 역추적, 네트워크 보안, iTrace

I. 서 론

오늘날 인터넷이 지식 정보화 사회의 기반이 됨에 따라 네트워크 공격의 수가 급증하였다. 최근 공격은 에이전트화, 분산화, 자동화, 은닉화 되는 특징을 보이는데 이는 공격 기법 또한 발전하였기 때문이다. 이렇게 공격 기법이 갈수록 발전하는 이유는 현재의 네트워크 환경에서는 공격에 대해 추적이 거의 불가능하기 때문에 공

* 한남대학교 컴퓨터공학과

접수일자 : 2007. 3. 6

격자는 안심하고 공격을 할 수 있기 때문이다.

현재 네트워크 보안 관리는 방화벽(firewall), 침입탐지시스템(Intrusion Detection System)과 결합해서 자신의 도메인 상에서만 공격을 탐지하고 보호하는데 초점이 맞추어져 있다. 하지만 최근의 공격의 많이 시도되고 있는 DDoS(Distributed Denial of Service) 같은 경우 공격은 거짓 공격자 주소를 사용하여 에이전트화, 분산화, 자동화 되어 여러 네트워크를 경유하여 목표 시스템을 공격한다. 이러한 이유로 해당 공격에 대해서 차단하더라도 다른 네트워크를 경유하여 제2, 제3의 공격이 가능하다.

본 논문에서는 이러한 공격에 대해 자동화된 실시간 역추적 기술을 적용한 능동형 보안 시스템을 제안하여 좀 더 안전한 네트워크 환경을 이루고자한다. 논문의 구성은 다음과 같다. 2장에서는 능동형 보안을 위한 능동 보안 기술에 대해 소개한다. 3장에서는 침입자 역추적을 위한 IP 역추적 기술에 대해서 소개한다. 4장에서는 침입자 역추적을 위한 능동형 보안 프레임워크를 기술하고 5장에서는 제안 시스템에 대한 실험과정과 결과에 대해 기술한다.

Ⅱ. 능동 보안 기술

능동 보안 기술에서의 능동이란 보안 측면에서 네트워크 침입에 대한 능동적인 대응을 의미한다. 능동적인 대응은 주로 침입자에 대한 역추적(traceback)과 침입자의 트래픽에 대한 대응(blocking, isolation 등)에 주안점을 갖는 것을 의미한다. 따라서 능동 보안이란 공격자를 추적하여 공격자가 접속해 있는 네트워크의 접속점을 차단하거나, 보복 공격을 할 수 있도록 하는 능동형 보안 기술을 총칭한다[1].

본 논문에서는 능동보안 기술과 관련하여 IETF에서 제안하는 "ICMP Traceback Message" 기술을 이용한 능동적인 보안 시스템을 제안한다. 또한 제안 시스템은 기존의 수동적인 보안 시스템의 문제점을 극복하고 능동 보안 기술을 만족하기 위해 다음 사항을 만족한다.

표 1. 능동 보안 시스템 요구 사항
Table 1. Active security system requirement

능동 보안 시스템 요구 사항	
확장성	다양한 유형의 서비스 수용을 위한 유연한 확장성
실시간	침입에 따른 실시간적인 대응
적응성	기존 네트워크 변경 없이 적용
능동형 공격 대응	공격자의 위치의 역추적을 통해 능동적인 대응 제공
보안 관리 영역간의 연계	단일 네트워크뿐 아니라 네트워크간의 연계에 의한 글로벌 네트워크 차원에서의 대응 방안 제공

표 1의 요구 사항을 만족함으로써 보안 환경 변화 및 보안 정책에 신속한 적응성을 가질 수 있고 에이전트와 서버와의 상호 연계를 통해 우회적인 사이버 공격, DDoS 공격과 같은 무차별적인 공격에 대응할 수 있는 능동형 보안 시스템을 만족하고자 한다.

Ⅲ. IP 역추적 기술

3.1 확률적 패킷 마킹 기반의 역추적 기법

확률적 패킷 마킹 기법(PPM: Probabilistic Packet Marking Scheme)은 네트워크를 순회하면서 지나간 라우터의 IP 주소를 패킷 속에 삽입하는 방식으로 마킹된 패킷을 받은 호스트는 라우터 주소 정보를 이용하여 지나온 경로를 재구성 할 수 있게 한 것이다. 일반적으로 패킷 마킹은 IP 헤더의 Record Route option 필드나 Identification 필드를 이용하여 라우터의 주소를 저장하는 방식으로 Node Append, Node Sampling, Compress Edge Fragment Sampling 기법 등이 있다[2][3][4].

3.2 호스트 기반의 역추적 기법

호스트 기반의 연결 역추적 기술은 역추적을 위한 모듈이 인터넷상의 호스트들에 설치되는 역추적 기법으로 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술이다. 그러나 이러한 방법을 이용하여 역추적을 수행하기 위해서는 인터넷상의 모든 호스트에 역추적 모듈이 설치되어야 하고, 역추적 경로 상의 단 1개의 시스템에서라도 어떤 문제에 의해서 역추적 정보를 얻을 수 없게 되는 경우가 발생하

면 역추적이 불가능하게 되는 단점을 가지고 있다[5][6].

3.3 네트워크 기반의 역추적 기법

네트워크 기반의 역추적 기법은 네트워크상에 송·수신되는 패킷으로부터 역추적 정보를 얻어 근원지를 역추적 하는 기법이다. 이러한 네트워크 기반의 역추적 기법으로는 SPIE(Source Path Isolation Engine), SWT(Sleepy Watermark Tracing) 등이 있다[7][8].

Ⅳ. 능동형 보안 시스템 프레임워크

본 논문에서 제안하는 능동형 보안 시스템 프레임워크에서 IP 역추적을 위하여 IETF가 제안하는 iTrace Message(ICMP Traceback Message)를 이용하며, 각 지역 네트워크에 에이전트가 설치되며 관리 네트워크에 서버가 설치된다. 각 지역 네트워크에 설치된 에이전트는 역추적 시 iTrace Message를 생성하여 서버에 전송하게 되고 관리 네트워크에 설치된 서버는 각 지역 네트워크에 설치된 에이전트들로부터 수신한 iTrace Message를 이용하여 침입자 역추적을 수행하게 된다. 그림 1은 본 논문에서 제안한 역추적 시스템 서버와 에이전트가 설치된 네트워크 구조이다.

에이전트는 네트워크에 전략적으로 배치되어, 네트워크 세그먼트들 사이에 분산 네트워크 구역을 제공하고 에이전트들로부터 전송받은 iTrace Message를 이용하여 공격자 근원지를 역추적 할 수 있다. 이 기능은 같은 도메인 안에 놓인 네트워크에서 DDoS 침입에 대응하여, 즉각적이고 자동적으로 역추적 기능을 수행할 수 있다. 이미 확보된 공격패턴에 의한 침입은 물론, 침입자가 위장 IP 주소를 사용하여 침입을 시도하게 되면 이상 탐지 이벤트가 프로토콜 상태가 왜곡된 것을 감지하고, 공격이 시도된 패킷들을 가려낸다. 이러한 이벤트들에 의해 확보된 정보들을 기반으로 침입 또는 공격의 중요도를 결정하여 관리 모니터에게 전달하면, 해당 에이전트가 속한 세션은 침입시도를 받은 시스템들로부터 안전하게 분리시키고, 필요에 따라 상부 프로바이더에게 정보를 전송하기도 한다. 이런 침입자에 대한 고립화 정책은 침입을 근원적으로 고립시켜 결국 시도자체를 중단시키게 된다.

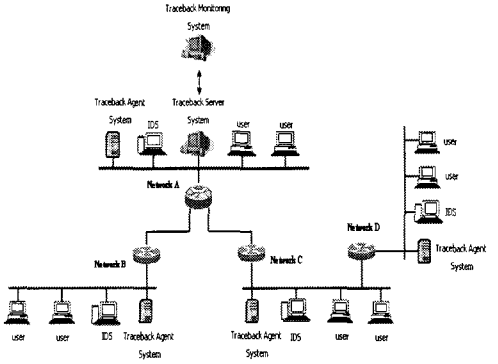

그림 1. 역추적 서버/에이전트가 설치된 네트워크 구조
Fig. 1. The network architecture with traceback server/agent

4.1 iTrace Message 구조

제안 시스템에서 IP 역추적을 위해 사용하는 iTrace Message는 ICMP의 형태로 그림 2와 같은 구조를 지니고 있다. 메시지는 ICMP 형태의 ICMP 패킷을 전달한다. 이때 코드 필드는 항상 0(no code)으로 설정되어 있어야 하고 수신자는 반드시 이를 허용 해야만 한다. 각 element 형태의 VALUE는 하나 또는 그 이상의 TYPE-LENGTH-VALUE(TLV) 형태를 가질 수 있다. TYPE 필드는 상위 element가 0x01에서 0x7, 하위 element가 0x81에서 0x87의 범위를 가진다[9].

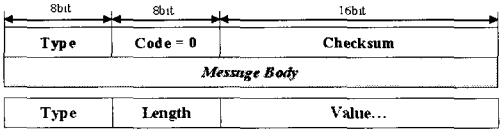

그림 2. iTrace Message 형태
Fig. 2. iTrace Message format

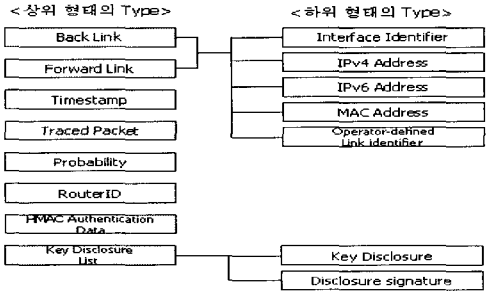

그림 3. iTrace Message 정의
Fig. 3. iTrace Message definition

여기서 상위 필드의 Forward Link와 Backward Link는 역추적 패킷에 대한 이동경로를 제공하고 iTrace Message 연결 구성을 위한 경로 정보를 제공하게 된다. 그리고 공격자에 의한 위조 iTrace Message를 방지하기 위해 전자서명의 인증 기술을 사용하는데 여기서는 HMAC 인증을 사용한다. HMAC 알고리즘은 MD5와 SHA-1 모두 지원하며 제안 시스템에서는 SHA-1 알고리즘을 사용한다.

4.2 에이전트 시스템 구조

에이전트는 각 지역 네트워크에 설치되어 네트워크 트래픽 수집, 패킷 분석, iTrace Message 탐지, iTrace Message 생성, 비정상 패킷 처리를 수행하게 된다.

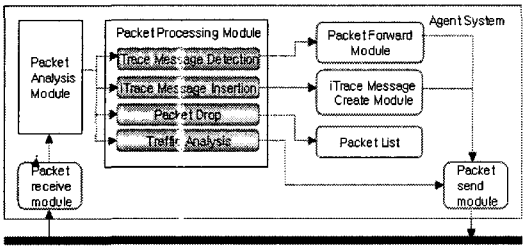

그림 4. 에이전트 시스템 구조
Fig. 4. Proposed agent system

패킷 수신 모듈은 지역 네트워크의 패킷들을 수신하여 패킷 분석 모듈로 전송한다. 패킷 분석 모듈은 수신한 패킷을 분류하여 iTrace Message 탐지, iTrace Message 생성, 비정상 패킷 처리, 트래픽 분석 모듈을 처리한다. 서버에서 iTrace Message 생성 명령을 수신하면 해당 패킷에 대해 iTrace Message를 생성하여 서버로 전송하게 된다.

iTrace Message 생성 절차는 다음과 같다. 공격자에 의한 위조 iTrace Message를 방지하기 위해서 서버와 에이전트는 비밀키를 서로 공유하게 된다. 이때 비밀키는 서버 측에서 생성하여 에이전트에게 전송되게 된다. 에이전트에서는 iTrace Message 생성 후 비밀키 K값을 이용하여 메시지 해시값을 생성하여 같이 서버에게 전송하게 된다. 서버는 iTrace Message 수신 후 에이전트와 공유한 비밀키 K를 이용하여 iTrace Message 해시값을 생성 후 에이전트에게 수신한 iTrace Message 해시값을 비교하게 된다.

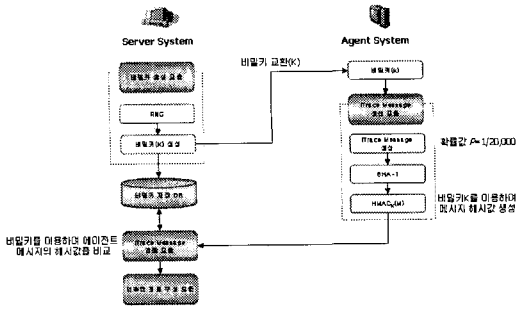

그림 5. iTrace Message create module
Fig. 5. iTrace Message create module

4.3 서버 시스템 구조

서버는 관리 네트워크에 설치되어 지역 네트워크에 설치되어 있는 에이전트로부터 iTrace Message를 수신하여 역추적 경로 구성을 수행하고 침입에 따른 정책을 에이전트들에게 전송하는 역할을 한다.

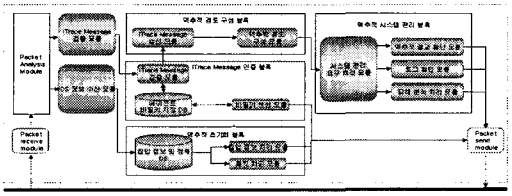

그림 6. 서버 시스템 구조
Fig. 6. Proposed server system

침입탐지 시스템에서 침입 정보를 수신하게 되면 서버 시스템은 해당 패킷에 대한 패킷 차단 정책을 각 에이전트에게 전파하고 iTrace Message 생성 명령을 송신하게 된다. 에이전트로부터 iTrace Message 수신 후 서버의 iTrace Message 인증 블록에서는 다음과 같은 과정을 통해 iTrace Message의 유효성을 검증하게 된다.

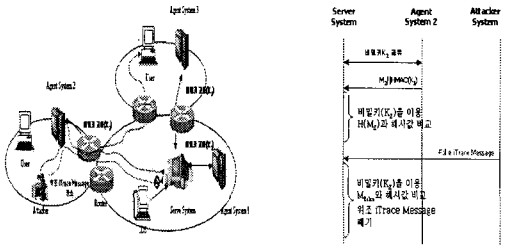

그림 7. 서버-에이전트 간의 비밀키를 이용한 iTrace Message 검증
Fig. 7. Validate iTrace Message using secrete key

먼저 서버의 비밀키 생성 모듈에서 각 에이전트들과 공유할 비밀키 Kn를 생성한다. 서버는 생성한 비밀키 Kn를 비밀키 DB에 저장하고 각 에이전트들과 공유하게 된다. 침입 발생 후, 에이전트로부터 수신한 iTrace Message의 유효성 검사는 이전에 교환한 비밀키 Kn을 이용하여 하게 된다. 그림 7은 공격자가 에이전트 2를 통해 위조 iTrace Message를 서버에게 전송하는 경우이다. 그러나 서버는 에이전트 2와 교환한 비밀키 K2를 이용하여 해시값을 생성하여 공격자가 보낸 위조 iTrace Message를 식별하여 폐기하게 된다.

4.3 iTrace Message를 이용한 경로 재구성

그림 8은 본 연구에서 설계된 해커의 공격에 대한 역추적과 대응, 그리고 역추적 결과를 통보하는 매커니즘을 보여주고 있다. 서버-에이전트 간의 비밀키는 서로 공유하고 있고 역추적을 위한 에이전트는 라우터에 모듈화 되어 있다고 가정한다. 에이전트는 모든 패킷에 대해 1/20,000의 확률로 iTrace Message를 생성한다.

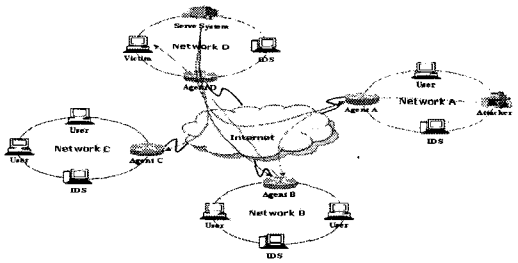

그림 8. 공격에 대한 역추적 대응
Fig. 8. IP traceback and response

네트워크 A내의 해커가 네트워크 D에 있는 시스템을 공격한다면 다음과 같은 역추적 과정을 거쳐서 대응 하게 된다.

단계 1. 네트워크 A내의 해커는 네트워크 D내의 호스트를 공격하기 위해서 네트워크 B를 경유한다.

단계 2. 해커는 네트워크 D내에 있는 호스트 공격을 시도한다.

단계 3. 네트워크 D는 공격을 탐지하고 침입 사실을 서버로 통보한다.

단계 4. 서버는 침입 사실을 네트워크 D에 있는 에이전트들에게 통보하고 네트워크 D의 에이전트는 피해 시스템을 목적지로 하는 패킷들에 대한 차단을 실행한다.

단계 5. 서버는 각 에이전트들로부터 수신한 iTrace Message의 유효성을 검증한다. 유효성 검증은 이전에 서로 공유한 서버-에이전트 간의 비밀키를 이용한다.

단계 6. 서버는 수신한 iTrace Message 중에서 Timestamp 값이 가장 큰 iTrace Message를 선택하여 RouterID에 대한 backward link와 forward link을 저장한다.

단계 7. backward link와 일치되는 forward link를 가진 iTrace Message 중에서 timestamp 값이 가장 차이가 적은 iTrace Message를 선택하여 연결체인을 형성한다.

단계 8. 일치하는 iTrace Message가 없을 때 까지 연결체인을 구성한다.

단계 9. 역추적 연결 체인 구성 후, 서버는 공격자 근원지를 파악하여 공격자에 대한 네트워크로부터의 단절 정책을 내리게 된다.

V. 능동형 보안 시스템 구현 및 성능 평가

본 논문에서 제안한 능동형 보안 시스템에서 에이전트는 현재 네트워크에서 사용하고 있는 라우터와 동일한 위치에 놓일 수 있다. 그러나 현재 라우터에 직접 사용자가 프로그래밍한 모듈을 탑재하기란 쉽지 않으므로 본 논문에서는 라우터에서 송/수신한 정보를 1차적으로 입력/출력 받을 수 있는 별도의 에이전트로 대체한다.

이때 에이전트는 차후 사용자가 리눅스 라우터로 대체가 가능할 수 있도록 운영체제를 RedHat 9를 사용하였고 커널 버전 2.6.12.5를 사용하였다. 그리고 에이전트의 개발 언어로써는 C언어를 사용하였고 컴파일러로 gcc egcs-2.91.66을 사용하였다. 서버는 Windows2003 Server기반에서 Microsoft Visual Studio .NET 2003을 사용하여 개발하였다.

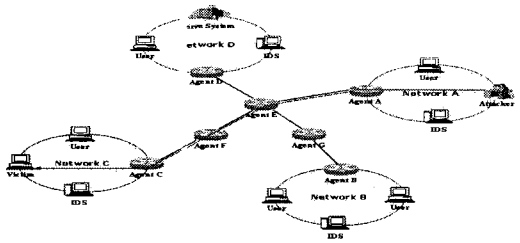

그림 9. 테스트 베드 구성 및 공격 경로
Fig. 9. Network configuration and attack path in experiment

본 논문에서 제안한 능동형 보안 시스템의 실험을 위해 그림 9와 같은 테스트 베드를 구축하였다. 공격자는 에이전트 A(라우터 A), 에이전트 E(라우터 E), 에이전트 F(라우터 F), 에이전트 C(라우터 C)를 거쳐서 피해 시스템에 DDoS 공격을 하게 된다.

공격에 대한 역추적 경로는 에이전트 A의 forward link와 에이전트 E의 backward link와 연결되고, 에이전트 F의 backward link와 에이전트 E의 forward link와 연결된다. 그리고 마지막으로 에이전트 C의 backward link와 에이전트 F의 forward link와 연결된다.

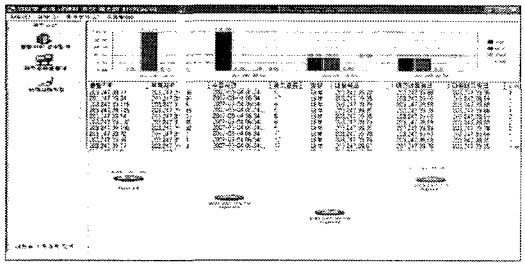

그림 10. 서버를 통한 IP 역추적 결과 확인
Fig. 10. Result of IP traceback at server system

그림 10은 테스트 베드에서의 공격에 대한 역추적 결과와 해당 에이전트에서의 트래픽 분석에 대한 결과를 보여주고 있다. 오른쪽 상단에는 패킷 분석을 통해 전체 네트워크에 대한 패킷별 현황을 그래프로 보여주고 있다. 그래프를 통해 다량의 UDP 패킷이 발생하였다는 것을 볼 수 있다. 그리고 각 패킷에 대한 분석 결과를 아래에서 상세히 보여주고 있다. iTrace Message를 이용한 공격자에 역추적 결과 값은 GUI 화면을 통해 확인할 수 있다. 공격자 역추적 후, 에이전트 A는 공격자를 네트워크로부터 차단하게 된다.

본 논문에서 제안한 능동형 보안 시스템은 관리 시스템의 부하가 적기 때문에 네트워크 부하 및 대역폭 부하가 적음에도 불구하고 역추적 가능성이 높은 편이다. 또한 iTrace Message에 인증 모듈 삽입했다는 점에서 보안 기능이 높은 편이고 현재의 네트워크 구조의 변경 없이 적용 가능하기 때문에 적용 가능성 높고 에이전트 시스템을 사용하기 때문에 확장성 또한 기존의 보안 시스템에 비해 높다고 할 수 있다.

VI. 결 론

본 논문에서는 기존의 수동적인 보안 시스템의 한계를 극복하기 위해 IP 역추적 기술을 이용한 능동적인 보안 시스템을 설계하고 구현하였다. 이렇게 제안된 시스템은 구현을 통하여 타당성과 정당성을 이론적인 방법과 실험적 방법으로 증명하였다.

능동 보안 기술로 기존에 제안된 역추적 시스템은 현재 인터넷에서 네트워크의 구조적인 변경 없이 적용이 불가능 하지만 논문에서 제안한 iTrace Message를 이용한 역추적 시스템은 네트워크의 구조적인 변경 없이 현재의 네트워크에 적용할 수 있다는 점과 차후 Agent System이 리눅스 라우터에 적용이 가능하도록 설계하고 구현하였다는 장점을 가지고 있다. 또한 기존에 제안 시스템에 비하여 관리 시스템의 부하와 네트워크의 부하가 적어서 제안된 능동 보안 시스템이 네트워크 트래픽의 원인이 되는 부작용을 줄일 수 있다. 또한 확장 가능성 또한 본 논문에서 제안한 능동 보안 시스템의 장점이라고 할 수 있다. 이렇게 설계되고 구현된 능동 보안 시스템은 현재 빈번하게 일어나고 있는 해킹으로부터 개인 또는 기관의 정보를 보호할 수 있다는 장점뿐만 아니라 해킹 시도 자체의 줄임으로써 좀 더 안전하고 깨끗한 인터넷 환경을 만들 수 있다.

향후 연구로는 제안 시스템의 제안한 능동 보안 시스템을 바탕으로 모바일 네트워크 및 Ad-hoc 네트워크 상에서의 공격에 대한 역추적이 가능한 능동 보안 시스템에 대한 연구가 필요하다고 볼 수 있다. 또한 이러한 능동 보안 시스템을 라우터가 포함하여 안전적인 서비스를 제공하는 방법에 대한 연구가 필요하다.

참고문헌

[1] "차세대 인터넷을 위한 능동 보안 기술 백서", 한국전자통신연구원, 2001

[2] 강동호, 한승완, 서동일, 장종수, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원

[3] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack", Proc. IEEE INFOCOM 01 pp 338-347, 2001.

[4] D. X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback", Proc. Infocom Vol2, pp 878-886, 2001.

[5] H. T. Jung et al. "Caller Identification System in the Internet Environment", 4th Usenix Security Symposium, 1993.

[6] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent", 1999 FIRST Conference, 1999.

[7] A.C Snoeren, C. Partride, 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.

[8] 서동일, "패킷 워터마크 기반의 인터넷 침입자 실시간 연결 역추적 메커니즘", 충북대학교대학원 이학박사학위논문, 2004.

[9] Steve Bellovin외 2명, "ICMP Traceback Messages", Internet Draft, IETF, Feb. 2003.

저자소개

김 재 동(Jae-Dong Kim)

1998년 한남대학교 컴퓨터공학 (공학석사)
2004년 ~ 한남대학교 컴퓨터공학 (박사과정)
※관심분야 : 네트워크 및 웹 서비스 정보보호

채 철 주(Cheol-Joo Chae)

2006년 한남대학교 컴퓨터공학 (공학석사)
2006년 ~ 한남대학교 컴퓨터공학 (박사과정)
※관심분야 : 네트워크 및 웹 서비스 정보보호

이 재 광(Jae-Kwang Lee)

1986년 광운대학교 전자계산학 (이학석사)
1993년 광운대학교 전자계산학 (이학박사)
1993년 ~ 한남대학교 컴퓨터공학과 교수
※관심분야 : 네트워크 및 웹 서비스 정보보호