情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

역추적 기술의 동향 및 적용 사례 분석

김 태 봉*, 최 운 호**

요 약

본 연구는 인터넷 사용자의 증가와 사용 환경이 급성장하는 가운데 유해성(각종 사이버테러 등) 역시 증가하고 있다는 문제점과 대응을 분석하였다. 이러한 상황에서 각종 정보보호시스템이 개발되어 운용되고는 있으나 현재 까지 역추적 기술에 대한 완벽한 대안을 제시하고 있지는 못하고 있다. 해킹이 시도된 후 이를 막기 위한 제품/서비스로 해킹 시도 자체를 방지하는 데는 한계를 가지고 있다. 따라서 적절한 실시간 역추적 기술의 도입을 통해 기존 네트워크 체계의 문제점을 해결하고 보안성을 극대화 할 수 있을 것이다. 본 연구에서는 실시간 역추적 기술의 동향과 적용 사례 분석을 통한 이해와 개념을 제시한다.

Ⅰ. 서 론

역추적 기술의 등장 배경은 사이버테러(해킹)의 증가와 은폐 및 위장 기술의 향상, 현재까지 로그분석을 통한 추적의 기술적 한계 봉착, 해외 프락시서버 경유 및 IP 스푸핑등 접속 위장시 사실상 추적의 불가능으로 인한 책임소재 파악 불명 및 원인 규명 어려움에 있다. IP역추적은 다음의 요인들에 의해서 필요성이 제기되고 있다.

경제성(추적에 소요되는 비용과 시간, 노력)의 향상, 과학적이고 기술적인 원인 규명과 오대응 방지, 위협의 실체 파악에 따른 대응안 강구 및 침입 재발 방지, 심리적 압박을 통한 예방효과 증대 및 사고발생 시 분석, 법률적 증거(Forensics) 강화 및 책임 소재 규명에 있다.

역추적 기술은 일반적인 'Log분석'의 한계를 극복하고자, 다양한 이론과 기법이 연구되었으나 대부분 실용성이 없거나 경제성이 없었다. 이는 'TCP/IP' 구조란 틀에 얽매임에 기인하기도 한다.

최근의 역추적 기술 추세는 실용성과 경제성 그리고 합법성을 보장하는 '플러그인 기법'이 주류를 이루고 있으며, 일부 불법적인 방법인 취약성을 겨냥한 기법은 '패치'로 인해 성공률이 낮으며 PC방화벽 등에 의해 대부분 탐지 및 제거되어 실용성이 없다.

이러한 최신 '역추적 기술'의 기술적인 요구 사항은 추적시스템은 독립적으로 구성되며 특정 매개체(추적을 위해서 무엇을 반드시 설치 해야만 한다는 것 등)를 요구치 않을 것, 실용적이고 현실적으로 즉각 적용 가능하며, 합리적인 비용이 제시될 것, 실시간 자동 추적 및 모니터링이 가능할 것, 추적의 기술적인 범위는 '우회경로'(프락시서버 등)를 초월하여 추적 대상자가 속한 게이트웨이(리얼 IP)와 실제 접속에 사용된 클라이언트(가상 IP)까지 추적할 것, 신뢰수준의 정확성(실제 적용시 99% 이상의 정확성)을 보장할 것, 현행법을 준수할 것("추적을 위해 해킹이나 취약성을 이용해서는 안 됨")등으로 정리 할 수 있을 것이다.

Ⅱ. 어플리케이션 보안의 이해와 역추적 기술의 적용 가능성

최근 어플리케이션에 대한 보안 논의가 활발하게 진행되고 있다. 이는 기존 OSI 7 Layer에서 점차 상위단계의 데이터 처리가 많아지고 있고 이에 대한 기존 보안체계의 한계로 기인한 바가 크기 때문이다.

예를 들어 어플리케이션이라 한다면, 웹 어플리케이션, 이메일, 메신저 등을 대상으로 한 각종 해킹, 웜

* (주) 아이자이어 로보텍스 대표이사 (pintech@naver.com)
한국정보보호학회 조기경보시스템연구회 WG18 "실시간 역추적 기술 연구" 운영자
** 금융결제원 금융 ISAC실 정보보호평가팀장 (tiger@kftc.or.kr)

과 바이러스, 유해 트래픽 등의 위험성 때문이며 이러한 위협이 내부정보유출, 각종 침해사고 등으로 나타나고 있는 게 현실이다. 그중 대표적인 어플리케이션 분야인 '웹어플리케이션'에 대해 알아보도록 하겠다.

1. 웹 어플리케이션 보안의 필요성

매일같이 언론보도를 통해 치명적인 웹 해킹 사고 사례 들이 보도되고 있는 현실에서, 웹의 개방적 속성상 항상 공격과 위협에 노출 되어있는 문제점을 갖고 있다. 이는 웹 취약성 공격법이 무분별하게 공개되어 있기 때문에 누구라도 손쉽게 공격자로 돌변할 수 있다는 문제를 지니고 있기 때문이다.

웹 기반 통합화에 따른 상대적 위협 역시 통합화되고 있고 이로 인한 위협의 증대가 초래되고 있으며 침입자는 웹 어플리케이션을 통해 WAS 및 내부 DB까지 접근 가능한 게 현실이다. 또한 웹 어플리케이션에 내재된 취약성이 존재하고 있고 지속 발생하고 있으며, 기존 보안 시스템(F/W, IDS 등)의 한계와 우회 가능성은 이미 입증된 바 가 있다. 마지막으로 해외 우회경로(프락시서버) 및 IP위장 시 추적불가로 침입이 재발되고 있다는 가장 큰 문제점을 지니고 있다.

2. 웹어플리케이션 해킹의 이해

웹 어플리케이션은 입력 값 검증 부재, 취약한 접근통제, 취약한 인증 및 세션 관리, 크로스사이트스크립팅(XSS), 버퍼 오버플로우, 삽입 취약점, 부적절한 에러 처리, 취약한 정보 저장 방식, 서비스 방해 공격, 부적절한 환경 설정의 대표적인 10대 해킹 유형이 존재한다. 이는 OWASP(Open Web Application Security Project)에서 정의한 바 있다.

이러한 10대 웹어플리케이션 해킹 유형이 URL커맨드 공격, 툴에 의한 공격, 웜과 서비스거부공격의 수단을 통해 OSI 7 Layer의 최상위 단계인 '웹어플리케이션' 계층을 공격한다는 특징을 가지고 있다. 그러면 왜 기존 보안체계로서는 이러한 위협을 막을 수 없는가이다. 방화벽의 경우 웹서비스가 이루어지는 80Port를 차단하면 웹서비스가 중단되기에 아무런 역할을 해줄 수가 없다. IDS의 경우 침입탐지 외에 차단을 할 수 없다는 기본적인 약점 외에도 어플리케이션 계층에 대한 침입탐지가 사실상 어렵다는 한계를 가지고 있다. IPS의 경우도 사실상 동일한 문제점을 지니고 있다. 즉, 웹어플리케이션 보안을 위해서는 기본적으로 웹어플리케이션에 대한 보안 정책과 매커니즘을 보유한 전문적인 제품을 통해서만이 가능하다는 뜻이다. 이를 위해 웹어플리케이션 보안 제품의 경우 어플리케이션 계층에 대한 실시간 대응(침입탐지 및 차단) 기능을 보유하고 있고, 어플리케이션 계층에서 실시간 패킷 조립 및 필터링을 통한 검사를 수행하고 있다. 그러나 이 경우에도 역추적이 불가능하다는 문제점이 제기되고 있어서 본 연구에서 이러한 문제의 해결방안을 제시한다.

3. 웹어플리케이션 보안에 적용하는 역추적 기술

웹어플리케이션 보안시스템 중 일부는 'Real Tracing'개념을 적용하여 역추적 기능을 구현하고 있다. 이러한 시스템은 'BPBT' 기법을 적용하고 있으며 이를 통해 실제 공격 근원지에 대한 실시간 모니터링을 가능하게 해준다. 통상적으로 웹어플리케이션 보안 시스템은 기존 방화벽이나 IDS, IPS에서 할 수 없는 웹 어플리케이션 레이어에 대한 보안을 위해 침입탐지 및 침입차단 기능을 제공하고 있다. 그러나 각종 공격 기법들이 지능화되면서 웜이나 DoS 등 로봇까지도 해외우회경로(프락시서버) 및 IP 위장을 통해 공격 근원지를 은폐하기에 효과적인 대응이 힘들었다. 이러한 문제를 해결하기 위해 최신 역추적 기법이 일부 사용되어 지고 있으며 이로서 호스트 및 네트워크 포렌식이 구현되고 있다.

Ⅲ. 웹어플리케이션 보안에 적용하는 역추적 기술

최근 인터넷 사용자가 급증하고 있는 인터넷상의 각종 범죄행위 또한 증가되고 있는 것이 현실이다. 대부분의 인터넷 트래픽은 웹 기반 국제적인 통신 규약인 HTTP(S)를 기반으로 하는 각종 웹 서비스에 집중되어 있다.

인터넷 침해 사고의 가해자들은 언제 어디서나 목적 대상인 웹서버에 손쉽게 접근할 수 있다. 인터넷 침해 행위자들은 개방형 구조인 웹서비스의 HTTP (S) 프로토콜을 통해 쉽게 웹서버를 공격하거나 각종 범죄행위를 저지르고 자신의 접속 지점을 간단히 은폐한다. 이는 접속 세탁을 위해 해외 프락시서버 등을 경유하여 IP 주소가 변조된다는 것에 착안한 것이다. 또한 많은 기업과 공공기관에서 가상사설망을 보편적으로 사용함에 따라 로컬 컴퓨터의 IP가 자동 은폐되므로 침해 행위자를 추적해 내기란 더욱 어려워지고 있다.

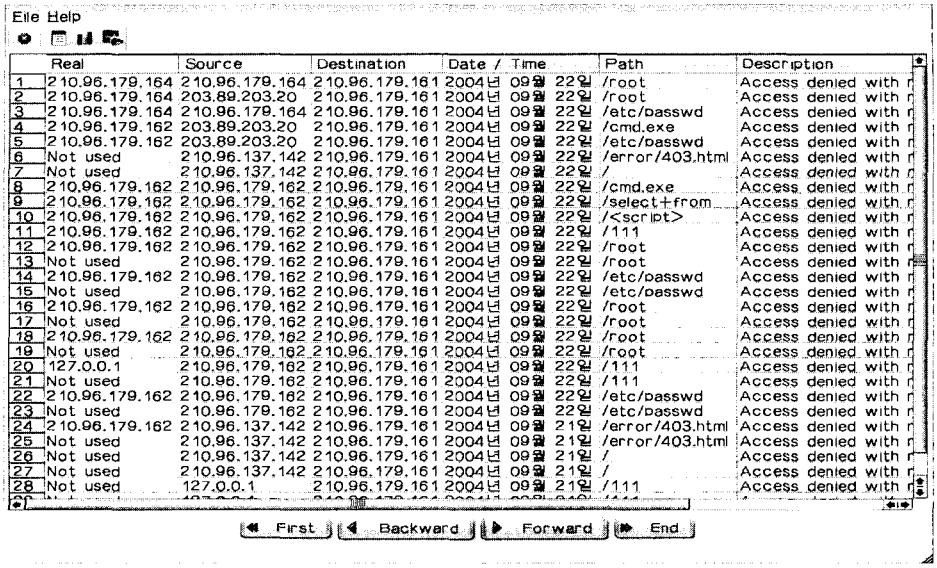


그림 1. 'Real Tracing' 추적 모니터링 화면(아이자이어로보텍스, 2004.9)

따라서 다단계로 접속 세탁이 된 침해 행위자라 하더라도 HTTP(S)를 통해 접속 연결을 시도하는 즉시 로컬 컴퓨터의 IP 주소와 내장된 각종 설정 값 그리고 각 경유지의 IP 주소까지 포함하여 자동으로 추적하여 실제 접속 지점에 대한 IP 차단 및 이력 관리를 실시 할 수 있고, 필요시 법률적 증거 제시 및 검거까지 가능하게 된다.

종래의 IP 주소 추적 시스템은 로그기록 파일에서 접속 기록을 읽어드려 IP 주소를 확인하였으나 TCP/IP 구조적 한계로 인해 직전 단계의 IP 주소 정보만 확인할 수 있다는 분명한 제한점을 가지고 있었다. 이러한 문제를 해결하고자 자바 애플릿 기반이나 Active-X 기반의 IP 주소 추적 시스템이 등장하였으나 다단계 추적이 가능하고 로컬컴퓨터의 IP 주소까지 확보한다는 개선점은 가졌으나 구조적 한계로 인해 팝업창 차단 및 PC 보안 프로그램 등에 의해 대부분 차단되어 활용성이 극히 낮다는 문제점을 내포하고 있다. 예시로 최근에 출시된 MS윈도우 XP 서비스팩2는 팝업창 차단 및 유해 차단 필터링 등의 PC 보안 기능이 기본 설정되어 있어 자바 애플릿 기반이나 Active-X 기반의 IP 주소 추적시스템은 동작할 수가 없게 되었다. 또한 자바 애플릿 기반 또는 Active-X 기반의 경우 웹서버의 HTML 페이지내에 스크립트 코드 형태의 에이전트를 포함할 수밖에 없는 구조로, 이 때문에 HTML 에러페이지 혹은 대상 페이지 모두의 소스를 각각 수정하여 삽입하여야 하는 불편함과 위험성을 내포하고 있다.

1. 'BPbT' 역추적 기술의 구조

상기와 같은 종래의 문제점을 해결하기 위하여 모니터링서버를 보호 대상인 웹 서버 및 네트워크 시스템과 통신 연결하고 제어 조건을 설정한 후 동작하며, HTTP(S)를 통해 접속 연결을 시도하는 로컬 컴퓨터의 웹브라우저 플러그인을 강제 구동케하여 접속 위치 변조 시라도 실제 IP 주소와 내장된 각종 설정값을 모니터링서버가 추적하고 관리할 수 있게 한다. 로컬 컴퓨터의 자체 보안 기능에 위치 추적이 차단되는 것을 방지하기 위해 PC의 보안 기능으로는 차단이 불가능한 웹브라우저의 플러그인을 구동시켜야 하며 이때 소켓통신을 통해 모니터링서버로 위치 정보 등을 전송한다.

또한 위치 추적을 위해 웹서버의 특정 HTML 페이지에 추적을 위한 코드를 내장하지 않고 원격지의 모니터링서버에서 직접 송수신 및 제어를 하는 위치 추적 시스템 및 방법을 제공하는데 그 목적이 있다.

웹어플리케이션 보안에 적용하는 역추적 기술은 '브라우져'는 '플러그인'을 기본적으로 탑재하고 있으며, '플러그인'의 종류는 약 100여종(VM, 플래시 등)에 이르고 계속 증가추세에 있다는 점에 착안하였다.

'브라우져'는 표준화된 도구로 정착되었고 IE, 넷스케이프, 아웃룩 등 다양성과 호환성을 보유하고 있으며 침입 탐지 및 사전 입력된 정보에 의거 추적 대

상자 선정시 '추적 시스템'에서 추적 모듈이 수행된다는 특징을 가지고 있다. 기술적인 매커니즘은 '브라우저'의 '플러그인'에 구동 명령을 전송하여 '소켓통신'을 생성하고 은폐한 IP 정보값 을 획득한다.

추적을 위해 클라이언트에 파일전송이나 설치를 않고 일체의 퍼미션을 초과치 않아 적법하며 스파이웨어나 'Active-X', Script등의 형태가 아니므로 보안창에 적발되지 않아 은밀성을 제공한다는 잇점을 지니고 있다. 이에 본 연구에서 다루는 'BPbT'(Browser Plug-in Based Tracing) 시스템은 'Real Tracing'이 구현된 것으로, 기존 호스트기반 'JBPA' 역추적 기법이 호스트에 국한되며 JVM만 지원한다는 한계를 극복하기 위해 등장하였다. 이는 호스트 기반인 'JBPA'의 기능과 장점을 그대로 계승하면서 네트워크상에서의 역추적을 지원하고 추적성공률도 월등히 개선시키기 위한 노력의 일환으로 창안되었다. 이를위해 'BPBT'는 웹브라우저 플러그인을 중심으로 JVM이외에 Flash와 같은 범용적이고 사용빈도가 절대다수인 플러그인을 지원하는 기능이 추가되었으며, 'BPBT'가 탑재된 네트워크 장비 혹은 서버가 HTTP 혹은 HTML을 지원하는 각종 패킷 및 데이터 영역에 역추적 명령을 강제케하는 컴포넌트가 내장된 것이 특징이다. 이러한 명령을 수신한 웹브라우저는 자동으로 해당 플러그인이 이를 인식하여 소켓통신을 생성하고 이때 내재된 각종 정보(클라이언트의 각종 정보 및 IP 값 등)가 자동으로 역추적서버에 도달하게 되는 것이다. 이로서 역추적을 위해 클라이언트측에 일체의 파일을 설치하거나 Active-X와 같은 스크립트를 사용하지 않아도 역추적이 가능해진 것이며 사용되어지는

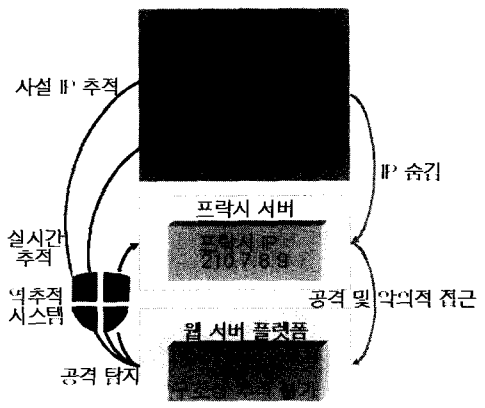


그림 2. 'Real Tracing' 추적기법 기능 구조
(아이자이어로보텍스, 2004. 9)

플러그인의 구조상 클라이언트측의 퍼미션을 초과하지 않으므로 혹시라도 제기될지 모르는 개인정보침해 및 유출과도 무관한 구조라 할 것이다. 이러한 기술을 응용한 제품군으로서 역추적을 기반으로 하는 '웹어플리케이션 보안 시스템', '바운싱백 방식의 스팸메일 방지 시스템', 'e-Mail 유통 경로 추적 시스템', '웹컨텐츠 및 계정접근 추적 시스템', '실시간 역추적을 통한 전자결제시 부인봉쇄 시스템' 등 다양한 분야에 적용이 가능한 것이 특징이라 할 것이다.

2. 'BPbT' 역추적 시스템의 구성도 및 역추적 기술의 발전방향

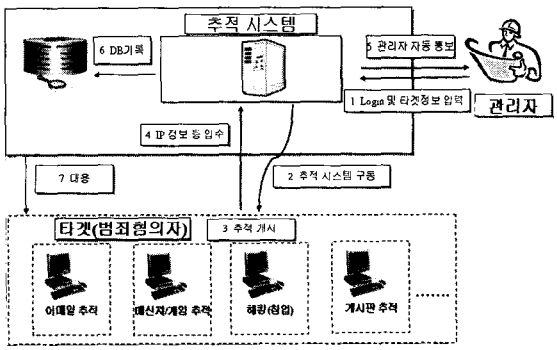


그림 3. 'BPbT' 역추적 기술의 구성도
(아이자이어로보텍스, 2005. 1)

3. 'BPbT' 역추적 기술의 실제 적용 사례

본 연구에서는 'BPbT' 역추적 기술에 대한 실제 적용 사례로 '웹어플리케이션 보안'의 예를 들었다.

이는 시장성측면에서 향후 보안 분야에서 가장 각광받고 있는 분야라는 특징 이외에도 기술적인 접근과 적용시 가장 큰 효과를 가져 올 수 있다는 긍정적인 면을 내포하고 있기 때문이다.

이를 통해 실시간으로 모든 침입과 접근을 역추적하여 공격근원지에 대한 색출과 대응이 가능하다는 장점을 보유하고 있으며, 아울러 선행 작업이 필요없다는 특장점과 현행 시스템과 네트워크에 부하없이 동작한다는 강점을 지니고 있는점이 매력적으로 작용 할 것이다.

Ⅳ. 결 론

본 연구에서는 역추적 기술의 정의와 필요성, 그리고 기존까지 연구가 진행된 기술의 분류와 새로운 가

표 1. 'BPbT' 역추적 기술의 발전방향

구분	1세대	2세대	3세대
시기	과거 (2000~2003)	현재(2004)	미래(2005~)
추적 성공률	최소 40~80% 수준	최소 80~99% 이상	99.9% 이상
종단 추적 방식	'PopUp' 방식	'Redirection' 방식	'능동형' 방식
특징	단일 플러그인 (VM) 지원	지원 '플러그인' 증가, 'Remote 추적' 지원, 추적 속도 및 정확성 향상	인공지능 부여 및 'BPBT' 이외의 추적기법과 결합
플랫폼	Java 및 관련 언어로만 구동 (역해석 약점)	Linux 기반 라이브러리 형태로 추적 체계 구현	장비형태로 구성(ASIC 등)
추적 회피 여부	PC방화벽에 차단됨	PC방화벽 차단 회피 가능	고도화
제한점	- 'VM'미지원시 추적 안됨 - 터미널은 추적 안됨 - 팝업 차단시 추적 안됨	- 터미널은 추적 안 됨 - 지원되는 플러그인 없을시 추적 안 됨	- 하이브리드 형태로 추적 강화 방안 강구

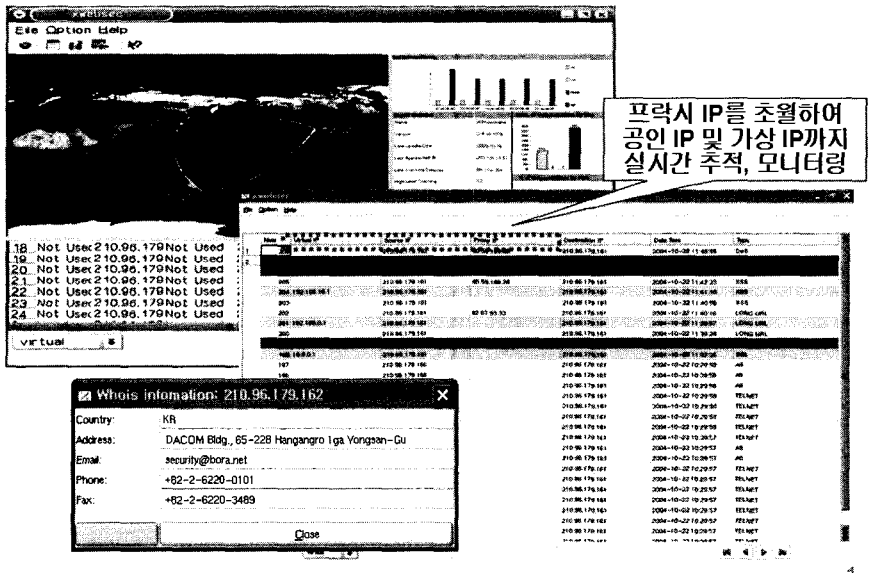


그림 4. 'BPbT' 역추적 기술의 적용 사례: 모니터링 화면(아이자이어로보텍스, 2005. 1)

능성(웹어플리케이션 보안 분야 적용)에 대한 고찰을 하였다.

이러한 최신 역추적 기술의 적용 분야는 각종 보안 관리 및 Forensics에 1차적으로 적용할 수 있을 것이다. 예를들어 통합 보안관리 시스템 및 조기경보시스템, 웹 어플리케이션 보안 시스템, 바운싱백 방식 스팸방지 및 추적, 이메일 정보유출 경로 추적 시스템, 인터넷 게시판 보안 및 계정 보안 시스템, 전자결제 시스템 보안: '부인 방지 및 봉쇄 효과'에 적용할 수 있을 것이다. 수사분야에 적용할 경우 사버범죄 수사용도의 이메일, 인터넷 게시판, 메신져 등 용의자를 추적할 수 있는 다양한 수단을 통합하여 자동화된 동작과 관리가 가능할 것이다. 추가적으로 정보전(Information Warfare)의 핵심 요소로서 사이버테러 및 사이버전에 대비 방어와 공격에 필수적인 요소인 정확한 '적'의 위치를 파악하여 정밀 대응토록 하며 각종 Defence 수단과 연계하여 정밀 타격 수단을 견지할 수 있다는 장점을 지니고 있다. 따라서 민.관.군 모든 분야에 두루 적용 가능한 효용성을 지니고 있고 현재 일부 상용화가 진행된 상태이므로 저변확대가 이뤄질 경우 국가적으로 큰 가능성과 경제적 이익, 보안성 향상의 효과를 기대할 수 있을 것이다.

참 고 문 헌

[1] 최운호, "국가 조기경보시스템 활성화를 위한 제안", 월간사이버시큐리티, 국가사이버안전센터 2004.5

[2] 김태봉, "HTTP(S) 보안을 위한 자동위치 추적 시스템 및 그의 방법", 아이자이어 로보텍스(특허출원 10-2004-0070329), 2004. 9월

[3] 김완수, "메일수신자 위치 추적 시스템 및 그의 방법", 트라이옵스(특허등록 10-0440270-0000), 2004. 7월

[4] 최양서, 서동일, 손승원 "역추적 기술 동향: TCP Connection Traceback 중심" ITFIND 주간기술동향 2003년 1월, http://kidbs.itfind.or.kr

[5] 전규삼, 최운호, "자동화된 침해대응시스템에서 Web을 기반으로 한 로봇에이전트에 대한 연구" 한국정보보호학회 하계학술대회, 2004년

[6] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent," FIRST Conference on Computer Security Incident Handling & Response 1999.

[7] 이준엽 외 4인, "IP역추적을 위한 새로운 접근 : 패킷손실기반의 논리적 전송경로 추정" 한국정보보호학회 논문지, 제12권 3호, 2002. 6.

[8] 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.

[9] 김병룡 외 3인, "마킹알고리즘기반 IP역추적에서의 공격근원지 발견기법" 한국정보보호학회 논문지, 제13권 1호, 2003. 2.

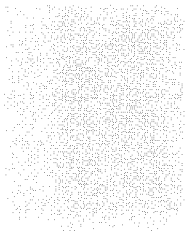
[10] 정종민 외 2인, "다중 에이전트를 이용한 역추적 시스템 설계 및 구현" 한국정보보호학회 논문지, 제13권 4호, 2003. 8.

[11] 이형우, "DDoS 해킹공격 근원지 역추적기술" 한국정보보호학회 논문지, 제13권 5호, 2003. 10

[12] www.ncsc.go.kr, "월간 국가/공공기관 해킹사고현황" 월간사이버시큐리티 8월호, 국가사이버안전센터 2004. 8

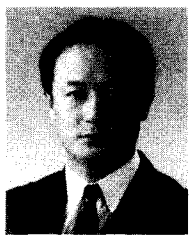
[13] 박종성, 최운호, 문종섭, 손태식, "자동화된 침해사고대응시스템에서의 네트워 포렌식 정보에 대한 정의", 한국정보보호학회 논문지, 4월, 2004년도

〈著 者 紹 介〉



김 태 봉 (Tae-bong Kim)

1997년 2월 : 세명대학교 경영학과 졸업
1995년 : 공저 '파워해킹테크닉'(도서출판 파워북 刊)
1996년 : 저서 '해커X파일'(도서출판 무당미디어 刊), 공저 '서세원 컴퓨터와 바람났네'(도서출판 한국컴퓨터매거진 刊)
1997년 : 저서 '해커와 보안'(도서출판 문화전사 刊)
2003년 2월~2004년 5월 : '(주)핀포인트 테크놀로지' 대표이사
2004년~현재 : '(주)아이자이어 로보텍스' 대표이사
2004년~현재 : 한국조기경보포럼 '역추적 기술 연구' 분과 운영자
〈관심분야〉 정보보호 및 정보전



최 운 호 (Un-Ho Choi)

1990년 : 광운대학교 학사
1995년 : 광운대학교 대학원 전자계산학과 석사
2004년 : 한세대학교 대학원 정보보호공학과 박사
1989년~1996년 : 한국전산원 선임연구원
1996년~2001년 : 한국정보보호진흥원 팀장
2002년~현재 : 금융결제원 금융ISAC실 정보보호평가팀장
2003년~현재 : 한국정보보호학회 이사
2004년~현재 : 한국정보보호학회 조기경보시스템연구회 위원장
2004년~현재 : 국가정보보안협의회 조기경보시스템연구회 위원장
〈관심분야〉 조기경보, 블랙리스트, 관제센터운영, 침해사고신고 자동화 등