論文
10-1-2

iTrace 메시지를 이용한 IP 역추적 시스템
IP Traceback System using iTrace Message

조한진(Han-Jin Cho)[1], 채철주(Cheol-Joo Chae)[2]
이준환(Lee June Hwan)[3], 이재광(Jae-Kwang Lee)[4]

요 약

최근 인터넷의 비약적인 발전으로 인하여, 해킹과 바이러스가 빠르게 퍼지고 있다. 이러한 역기능에 대응하기 위하여, 방화벽과 침입탐지시스템 같은 보안시스템이 개발되어 활용되고 있지만, 이러한 기법은 공격에 대한 한계점을 가지고 있어, 해킹 사고는 계속적으로 증가하고 있다. 이에 따라, 악의적 의도를 가진 침입자를 추적할 수 있는 자동화된 실시간 역추적 기법을 적용하여, 해킹 자체의 발생건수를 줄일 수 있는 방법에 대한 연구가 필요하게 되었다. 본 논문에서는 이러한 문제를 해결하기 위하여 IP 역추적 시스템을 제안하고자 한다. 역추적을 위하여 ICMP 형태의 역추적 메시지를 구현하고, 로컬 네트워크에 배치되는 에이전트와 관리 네트워크에 배치되는 서버 프레임워크를 설계하고, 능동형 보안시스템을 기반으로 침입자를 추적하고 고립화 하기위한 보안메커니즘을 구현한다.

Abstract

The rapid growth of the Internet has caused the hacking and virus. There are several vulnerabilities in current firewall and Intrusion Detection Systems 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.

논문 접수 : 2009. 1. 19.
심사 완료 : 2009. 2. 10.

1) 극동대학교 컴퓨터정보표준학부 교수
2) 한남대학교 컴퓨터공학과 박사과정
3) 극동대학교 컴퓨터정보표준학부 교수
4) 한남대학교 컴퓨터공학과 교수

※ 이 논문은 2007년 산학협동재단 학술연구비 지원사업에 의해 수행되었습니다

1. 서론

본 논문에서는 증가하는 해커들의 공격에 대해, 기존의 보안 시스템들과 같은 수동적인 개념이 아닌, 공격 시도 자체를 줄일 수 있는 능동적인 보안 시스템인 IP 역추적 시스템을 설계하고 구현한다.

역추적 시스템 모델은 서버-에이전트를 기반으로 하고, 역추적을 위한 메시지 기법인 iTrace 메시지를 사용한다. 에이전트 시스템은 기존 네트워크 구조에서의 라우터에 위치하며, 네트워크상의 패킷들을 감시하고 역추적 메시지를 생성하게 된다. 에이전트 시스템에서 생성한 역추적 메시지는 서버 시스템으로 전송되고, 이는 공격자 근원지 역추적에 사용된다. 서버 시스템은 각 에이전트 시스템에서 수신한 각 네트워크들에 대한 패킷 정보와 역추적 메시지를 이용하여, 분산 서비스 거부 공격과 같은 공격에 대한 근원지 역추적을 수행하게 된다. 또한 서버 시스템에서는 에이전트 시스템들로부터 수신한 패킷을 이용하여, 각 네트워크에서의 트래픽을 측정하여 이상 트래픽을 검출하게 된다.

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 IP 역추적 기술에 대해 소개하고, 3장에서는 침입자 역추적을 위한 IP 역추적 시스템 프레임워크에 대해 기술한다. 4장에서는 제안 시스템에 대한 실험과정과 결과에 대해 기술한 후 5장에서 결론을 맺는다.

2. IP 역추적 기술

2.1 패킷 마킹 역추적 기법

패킷 마킹 기법이란 네트워크를 순회하면서 지나간 라우터의 IP 주소를 패킷 속에 삽입하는 방식으로, 마킹된 패킷을 받은 호스트는 라우터 주소 정보를 이용하여 지나온 경로를 구성할 수 있게 한 것이다.

패킷 마킹은 TCP/IP 프로토콜 중에서 IP 헤더의 Record Route option을 이용하여, IP 헤더의 옵션 필드에 라우터의 주소를 저장하거나, IP 헤더의 Identification 필드에 라우터 주소를 저장할 수 있는 것을 활용한 기법으로, Node Append 기법, Node Sampling 기법, Compressed Edge Fragment Sampling 기법 등이 있다[1].

2.2 호스트 기반의 역추적 기법

호스트 기반 연결 역추적 기술은 역추적을 위한 모듈이 인터넷상의 호스트에 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 발생하면, 역추적이 불가능하게 되는 단점을 가지고 있다. 이와 같은 문제점들로 인해 현재의 인터넷 환경에 적용하는 것은 거의 불가능하다고 할 수 있다.

2.3 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[2][3].

2.4 어플리케이션 기반 역추적 기법

JBPA(JVM Based Plug-in Agent) 시스템은 "Real Tracing"이 구현된 것으로, 웹 브라우저 플러그인으로 사용되는 JVM을 이용한 역추적 기법으로, 호스트에 자바애플릿 형태의 에이전

트를 탑재하여, 접근하는 모든 사용자를 실시간으로 최초 접속지까지 역추적 할 수 있다는 장점을 가지고 있다.[4]

3. IP 역추적 시스템 프레임워크

본 논문에서 제안하는 능동형 보안 시스템 프레임워크에서, IP 역추적을 위하여 IETF가 제안하는 iTrace 메시지(ICMP Traceback Message)를 이용하며, 각 지역 네트워크에 에이전트가 설치되며 관리 네트워크에 서버가 설치된다. 각 지역 네트워크에 설치된 에이전트는 역추적 시 iTrace 메시지를 생성하여 서버에 전송하게 되고, 관리 네트워크에 설치된 서버는 각 지역 네트워크에 설치된 에이전트들로부터 수신한 iTrace 메시지를 이용하여 침입자 역추적을 수행한다. 에이전트는 네트워크에 전략적으로 배치되어, 네트워크 세그먼트들 사이에 분산 네트워크 구역을 제공하고, 에이전트들로부터 전송받은 iTrace 메시지를 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.

3.1 iTrace 메시지 구조

본 시스템에서 IP 역추적을 위해 사용하는 iTrace 메시지는 ICMP의 형태로 그림 3.1과 같은 구조를 지니고 있다. 이 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 0x07, 하위 element가 0x81에서 0x87의 범위를 가진다[5].

여기에서 상위 필드의 Forward Link와 Backward Link는 역추적 패킷에 대한 이동경로를 제공하고, iTrace 메시지 연결 구성을 위한 경로 정보를 제공하게 된다. 그리고 공격자에 의한 위조 iTrace 메시지를 방지하기 위해 HMAC 인증을 사용한다. MD5와 SHA-1 모두 지원하며, 본 시스템에서는 SHA-1 알고리즘을 사용한다.

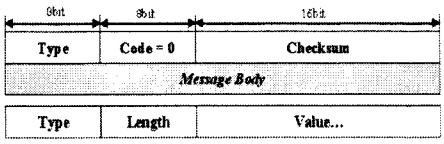

그림 3.1 iTrace 메시지 형태
Fig. 3.1 iTrace Message Format

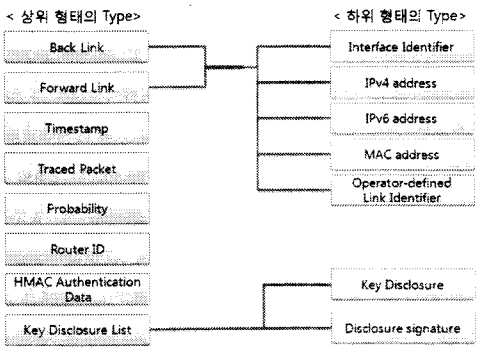

그림 3.2 iTrace 메시지 타입
Fig. 3.2 iTrace Message Type

3.2 에이전트 시스템 구조

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

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

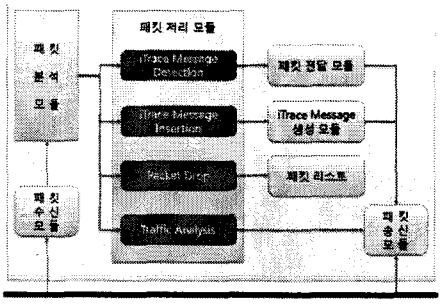

그림 3.3 에이전트 시스템 구조
Fig. 3.3 Agent System Architecture

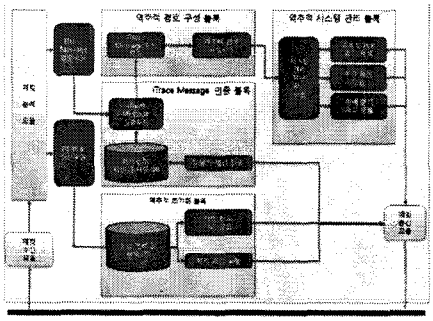

그림 3.4 서버 시스템 구조
Fig. 3.4 Server System Architecture

3.3 서버 시스템 구조

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

본 시스템에서 침입 정보를 수신하게 되면, 서버 시스템은 해당 패킷에 대한 패킷 차단 정책을 각 에이전트에게 전파하고, iTrace 메시지 생성 명령을 송신하게 된다. 에이전트로부터 iTrace 메시지 수신 후 서버의 iTrace 메시지 인증 블록에서는 iTrace 메시지의 유효성을 검증하게 된다.

3.4 iTrace 메시지를 이용한 역추적 경로 재구성

에이전트는 모든 패킷에 1/20,000의 확률로 iTrace 메시지를 생성하여 서버 시스템에 전송한다.

서버 시스템의 역추적 경로 구성 블록에서는 에이전트들로부터 수신한 iTrace 메시지를 이용하여 공격 경로를 재구성한다. 이때 역추적 경로 구성 블록에서는 iTrace 메시지의 Timestamp, Back Link, Forward Link를 이용한다. 그림 3.5는 이러한 역추적 경로 재구성 과정을 보여주고 있다.

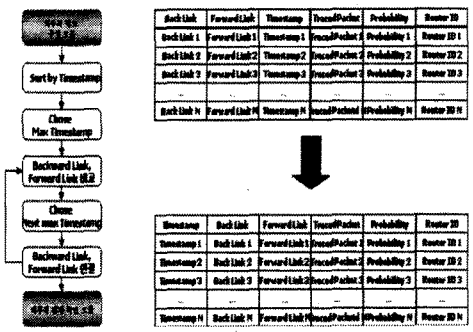

그림 3.5 역추적 경로 재구성 과정
Fig. 3.5 Traceback Route Reconstruction Process

단계 1) 수신한 iTrace 메시지 중에서 Timestamp 값이 가장 큰 iTrace 메시지를 선

택한다.

단계 2) 선택한 iTrace 메시지의 Back Link와 Forwa- rd Link가 일치하는 메시지를 선택한다. 다수의 iTrace 메시지가 있다면, Timestamp 값이 가장 큰 iTrace 메시지를 선택한다.

단계 3) 선택된 iTrace 메시지의 Timestamp 값과 가장 근접한 값을 가지는 iTrace 메시지를 선택한다. 단계 2의 과정을 반복한다.

단계 4) 더 이상 선택할 iTrace 메시지가 없을 때까지 단계 2~단계 3의 과정을 반복한다.

단계 5) 선택된 iTrace 메시지를 연결하게 되면 공격 경로를 재구성 할 수 있다.

4. IP 역추적 시스템 구현 및 성능 평가

그림 4.1은 nam 분석도구를 이용하여, 역추적 시뮬레이션 수행 결과를 보여 주고 있다. 설계한 실험환경에 따라 구축된 가상의 네트워크 환경에서, 공격 노드인 Node 0에서 피해 노드인 Node 7까지의 패킷이 전송되는 것을 보여주고 있다.

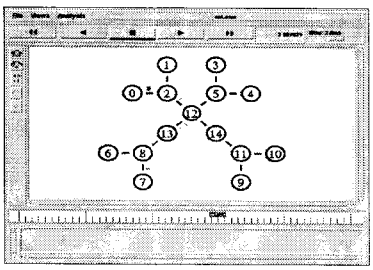

그림 4.1 역추적 시뮬레이션
Fig. 4.1 Traceback Simulation

그림 4.2는 GnuPlot를 이용하여 역추적 시뮬레이션 추적 파일 분석 결과를 그래프의 형태로 표현한 결과이다. 그래프에서 X축은 시뮬레이션 시간을 의미하고, Y축은 패킷을 송/수신하는 노드 ID를 의미한다. 패킷의 이동 경로는 두 가지의 형태를 보여주고 있다.

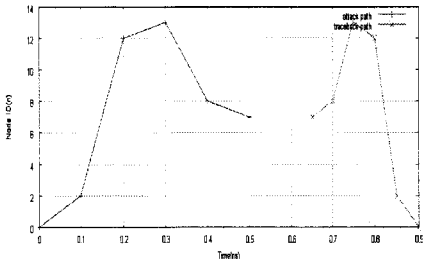

그림 4.2 패킷의 이동 경로
Fig. 4.2 Shifting Route of Packet

첫 번째는 공격 패킷의 이동 경로이고, 두 번째는 iTrace 메시지가 포함된 패킷의 이동 경로이다. 그래프에서 볼 수 있듯이, 공격 패킷의 이동 경로를 분석하면 최초 Node 0에서 시작하여 Node 2, Node 12, Node 13, Node 8을 경유하여 Node 7을 목적지로 하고 있다는 것을 확인할 수 있다.

공격에 대한 대응으로 iTrace 메시지가 포함된 패킷의 이동경로를 분석해보면 Node 7 → Node 8 → Node 13 → Node 12 → Node 2 → Node 0을 확인할 수 있다. 그러므로 최초 공격지인 Node 0을 역추적할 수 있다.

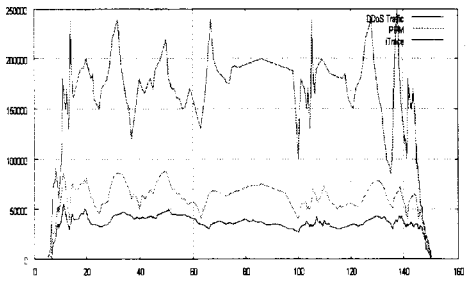

그림 4.3 제안한 시스템에서의 트래픽
Fig. 4.3 Traffic of Proposal System

그림 4.3은 DDoS 공격에 대해 PPM 방식과 제안 기법과의 트래픽을 분석한 결과이다. 기존의 패킷 마킹 기법은 DDoS에 대해, 각 라우

터에서 확률 p로 샘플링 하여 마킹하는 방식이므로, 그림 8에서 보는 바와 같이 DDoS 트래픽에 비례하여 생성되는 것을 확인할 수 있다. 본 논문에서 제안하는 방식은 이상 패킷에 대해 iTrace 메시지를 생성하여 전송하는 방식이므로, 기본의 PPM 패킷에 비해 많은 트래픽을 유발하지 않으며, 또한 iTrace 메시지가 전체 네트워크에 영향을 줄 수 있는 트래픽을 생성하지는 않는다는 것을 확인할 수 있다.

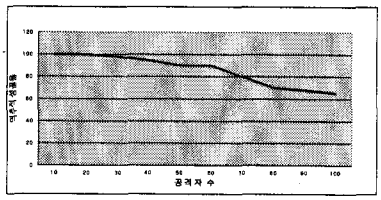

그림 4.4 제안 시스템의 역추적 성공률
Fig. 4.4 Traceback Success Rate of Proposal System

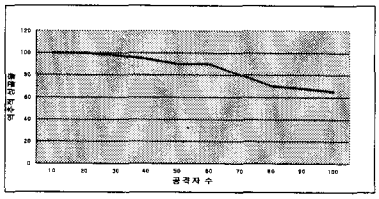

그림 4.4 제안 시스템의 역추적 성공률
Fig. 4.4 Traceback Success Rate of Proposal System

그림 4.4는 본 논문에서 제안한 시스템을 이용하여 랜덤으로 20회 DDoS 트래픽 기반 공격 시뮬레이션을 수행하였을 때 역추적 성공률을 보여주고 있다. 공격자의 수가 50개 이상일 때 성공률이 낮아지기 시작하며, 공격자 80개에 대해서 약 70%의 역추적 성공률을 보이는 것을 확인할 수 있다. 공격자 수가 80개 이상일 때부터 역추적 성공률이 낮아지지만 기관 내부 네트워크에 적용함을 고려하면 필수 시스템이라고 볼 수 있다.

[표 1]에서는 기존의 IP 역추적 기법들과 제안한 IP 역추적 기법들을 장점과 단점 부분을 비교해 보았다. 기존 기법에 비해 제안 기법은 실시간 가능성의 기능과 높은 역추적 성공률을 가지고 있으며, 향후 IETF의 표준화를 통해 확장성을 가지고 있다.

[표1] 제안 기법과 기존 기법 비교
[Table 1] Comparison Proposal System with other System

방식		장점	단점	비고
기존기법	수동 역추적	신뢰성 보장	시간소요	수사기관
	호스트기반	특정 도메인 내에서 빠른 역추적	·비표준 ·인터넷 환경에 적용하기 곤란	·비현실성
	네트워크기반	·역추적 성공률 높음 ·실시간 역추적 가능	·인터넷 환경에 적용하기 어려움	·비현실성 ·일부 네트워크에서 사용
	웹 애플리케이션 기반	웹 기반에서의 역추적 가능	·실행 코드 삽입 문제 ·법적인 문제	·수사기관과 공조 필요
제안기법	iTrace 메시지 이용	·역추적 성공률이 높음 ·실시간 역추적 가능 ·IETF 표준화 진행 중	·에이전트 배포 문제	

5. 결론

본 논문에서는 보안 요구사항을 반영하고 능동적인 대응을 수행할 수 있는 iTrace 메시지를 이용한 역추적 시스템을 제안하였다. 제안한 역추적 시스템은 공격이 종료되어도 공격자의 위치를 추적할 수 있으며, IETF에서 제안한 방식을 사용함으로서 표준화를 통해 확장성을 가지고 있다고 할 수 있다.

또한 본 논문에서 제안한 시스템은 네트워크의 구조적인 변경 없이 현재의 네트워크에 적용할 수 있다. 또한 기존 시스템에 비하여 관리 시스템의 부하와 네트워크의 부하가 적어서 제안된 능동 보안 시스템이 네트워크 트래픽의 원인이 되는 부작용을 줄일 수 있다. 확장 가능성 부분에서도 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 줄임으로서 좀 더 안전한 인터넷 환경을 만들 수 있을 것이다.

참 고 문 헌

[1] 이형우, "TTL 기반 패킷 마킹 방식을 적용한 IP 패킷 역추적 기법" 한국인터넷정보학회 논문지, 제6권, 제1호 pp 13-25, 2005.
[2] 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 Tech nical Memorandum No.1284, February 7, 2001.
[3] 서동일, "패킷 워터마크 기반의 인터넷 침입자 실시간 연결 역추적 메커니즘", 충북대학교대학원 이학박사학위논문, 2004.
[4] 최운호, 전영태, "대규모 컴퓨터 바이러스/웜 공격시 '종합침해사고대응시스템'에서의 자동화된 역추적 절차", 정보보호학회 학회지, 제15권, 제1호 pp 50-60, 2005년.
[5] Steve Bellovin외 2명, "ICMP Traceback Messages", Internet Draft, IETF, Feb. 2003.
[6] 강동호, 한승완, 서동일, 장종수, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원
[7] 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.
[8] D. X. Song, A. Perrig, "Advanced and Authenti cated Marking Scheme for IP Traceback", Proc. Infocom Vol2, pp 878-886, 2001.
[9] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent", 1999 FIRST Conference, 1999.

조 한 진

• 1999년 2월 : 한남대학교 컴퓨터공학과 (공학석사)
• 2002년 8월 : 한남대학교 컴퓨터공학과 (공학박사)
• 2002년 3월 ~ 현재 : 극동대학교 컴퓨터정보표준학부 교수
<관심분야> : 정보통신 및 응용서비스 정보보호

이 준 환

• 단국대학교 전기전자공학과 졸업(공학사)
• 단국대학교 대학원 전기전자공학과 석사 • 졸업(공학석사)
• 단국대학교 대학원 전기전자공학과 박사졸업(공학박사)
• 현 극동대학교 컴퓨터정보표준학부 교수
<관심분야> : 영상처리, 얼굴인식

채 철 주

• 2004년 2월 : 한남대학교 컴퓨터공학과 (공학사)
• 2006년 2월 : 한남대학교 컴퓨터공학과 (공학석사)
• 2006년 3월 ~ 현재 : 한남대학교 컴퓨터공학과 박사과정
<관심분야> : 네트워크 및 웹 서비스 정보보호

이 재 광

• 1986년 2월 : 광운대학교 전자계산학과 (이학석사)
• 1993년 2월 : 광운대학교 전자계산학과 (이학박사)
• 1993년 3월 ~ 현재 : 한남대학교 컴퓨터공학과 교수
<관심분야> : 네트워크 및 웹 서비스 정보보호