韓國 컴퓨터情報學會 論文誌
第8卷 第1號, 2003. 3.

2003-8-1-1-7

무선 방화벽의 설계 및 구현에 관한 연구

박 대 우*

A design and implementation of the Wireless Firewall

Dae-woo Park*

요 약

이동(Wireless & Mobile) 통신단말기 사용자가 내부 네트워크 안의 정보서버로 접속을 원할 시에, 불법적인 침입으로부터 무선네트워크의 자원을 보호하기 위해 무선 정보보안이 요구된다. 이동통신단말기의 무선네트워크에 접속 시 정보보호를 위해 유일한 경로에 설치된 무선방화벽이 필요하다. 본 논문에서 방화벽의 주요 기능인 패킷필터링, NAT(Network Address Translate), 인증, 무결성, 그리고 감사기록 기능들이 무선상태에서 이루어 지도록 무선방화벽을 설계한다. 그리고 무선방화벽상태에서 패킷필터링, NAT, 인증, 무결성, 그리고 감사기록 기능을 구현하고, 기능들을 확인한다. 그리고 무선방화벽의 연구개발을 위한 발전적인 제안을 통해 한국 무선방화벽의 기능향상과 성능개선에 도움을 주고자 한다.

Abstract

When Mobile terminal user want to contact inner-network information sever, wireless information security need for protect hacking. For the security, Mobile terminal user could have contact to wireless network through the gateway of Wireless Firewall. In this paper, I present a design scheme of Wireless Firewall that included major function of Packet Filtering, NAT, Authentication, and auditing reports services. I would implement to Wireless Firewall that included major function of Packet Filtering, NAT, Authentication, Integrity, and auditing reports services. I would conclude that the suggest will be useful for research and development on Korean Wireless Firewall System.

* 숭실대학교 컴퓨터학과 통신연구실

접수일자 : 2003. 1.20
심사완료 : 2003. 3. 8

Ⅰ. 서론

이동 기술을 바탕으로 한국 무선이동통신의 발전과 더불어 이동단말기의 전화 가입자 수는 2002년 9월말 기준 3200만명을 넘어서서 오는 2006년 4500만명에 이를 전망이다.[1] PCS, PDA와 IMT2000이 발전함에 따라 우리는 'Anytime, Anywhere, Anybody' 형태의 3A와 끊김없는(Seamless) 통신서비스 제공을 위해서 'Anynetwork, Anydevice, Anyservice' 개념을 추가한 6A 기반의 서비스가 요구된다. 그리고 이와 같은 서비스를 실현하기 위해서는 'Computing, Communica-tion, Connectivity, Contents, Calm' 등 5C 기술이 필수적이다. 따라서 차세대 이동통신 서비스는 현재의 네트워크에 더하여, 무선 통합, 홈 네트워크, 인체 네트워크, 마이크로 네트워크 등 다양한 통신 네트워크의 상호 연계를 통해서 모든 네트워크가 통합되면서 운용되는 유비쿼터스(Ubqiutos) 네트워크가 형성 될 것이다. 이때 단말기는 IPv6(Internet Protocol version6)를 통해 자신만의 고유한 주소를 갖게 되면서, 무선 네트워크에서 이루어지는 금융, 물류, 경영정보 등을 통해 정보교환 과 업무영역의 확대가 이루어질 것이다.

하지만 무선의 치명적인 약점인 이동단말기가 본인의 소유인지, 아니면 다른 사용자가 이를 부정적으로 사용하는 것인지에 대한 확인과 더불어 본인의 행위에 대한 부인방지(Non-repudiation)와 본인의 의사에 의한 사용자 인증을 받을 수 없다는 치명적인 약점이 있다. 따라서 무선영역에서 호스트로의 접속 및 정보전달 시에는 무선 방화벽으로부터 접속인증은 물론 불법적인 사용자에 대한 침입차단정책 및 무선정보 전달 체계에 대한 비밀성 유지가 요구되는 시대가 도래 되었다.

현재 네트워크에 연결된 시스템의 보안은 첫 출발점은 바로 방화벽이다. 방화벽은 외부와 내부 네트워크, 혹은 중요한 정보전송의 유일한 경로에 설치되어, 양자간에 오가는 모든 통신을 감시하여, 허용되지 않는 접근을 막는다.[2] 이로써 불법적인 네트워크 침입으로부터 내부 네트워크 시스템들과 중요한 정보자원인 호스트들을 보호한다. 따라서, 무선 방화벽을 게이트웨이에 설치하고, 사용자 인증과 침입차단을 통해서 무선네트워크에 중요자원을 보호할 수 있다.

본 논문에서는 방화벽의 보안성이 검증된 국가 인증 방화벽의 내용 및 방화벽의 목적과 기능을 파악하여, 이를 무선 상태에서 적용할 수 있도록 무선에서의 무선방화벽의 개념을 확정짓고, 한국에서의 무선 방화벽의 필요성을 확인하며, 이에 따른 무선방화벽의 목적과 기능에 맞게 설계를 하고, 이를 토대로 실험실 환경에서 구현하여 패킷필터링, NAT, 인증, 무결성, 그리고, 감사기록관리 기능을 구현하여, 무선방화벽의 기능이 작동됨을 확인 한다. 그리고나서 무선방화벽의 연구개발을 위한 발전적인 제안과 향후 연구계획을 제시하여, 우리나라 무선방화벽이, 세계에서 경쟁력을 갖춘 무선방화벽으로의 기능향상과 성능개선에 도움을 주고자 한다.

Ⅱ. 관련연구

1. 방화벽 보안성 인증

한국에서의 방화벽은 제품명으로는침입차단시스템이며, 정보보호제품으로써 보안성을 보증하기 위해 국가차원의 인증을 국가정보원에서 시행하고 있으며, 현재 2002년 8월 5일 정보보호시스템 평가인증지침(정보통신부고시 제2002-41호)을 시행하고 있다.[3]

침입차단시스템 평가기준은 보안기능의 신뢰성을 확인하기 위한 보증요구 사항으로 개발과정, 시험, 형상관리, 운영환경, 설명서, 취약성의 6가지 사항으로 이루어 진다. 평가등급은 K1 등급을 최저단계로 하고, K2, K3, K4, K5, K6 그리고 K7를 최고단계로 하여 총 7단계로 구분하고, 향후 국제표준의 ISO/IEC 15408-1의 원본인 국제공통평가기준[4]을 국내 표준으로 제정하여, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7의 7개의 등급으로 구분된다.[5]

현재 사용되는 K4인증 침입차단시스템의 일반적인 모델은 그림 1과 같이 하이브리드 듀얼 홈드게이트웨이 방식(Hybrid Dual-Homed Gateway)에다가 상태정밀검사 방식(Stateful Inspection)[6]을 도입하여 사용하고 있다.

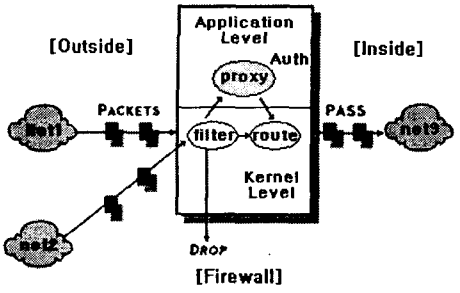

그림 1. 하이브리드 듀얼 홈드게이트웨어 방식
Fig. 1. Hybrid Dual-Homed Gateway

2. 방화벽 기능

정부에서 보안성이 검증된 K4 인증 방화벽[7]의 기능들을 크게 나누어 보면 다음과 같다.

2.1 패킷필터링(Packet Filtering)

방화벽에서는 패킷필터링 규칙을 설정하고, 이를 위반하는 패킷에 대해 접근 통제를 실시한다. 3계층인 네트워크층(Network Layer)의 IP(Internet Protocol)의 헤더(header)와 4계층인 전송층(Transport Layer)인 TCP(Transmission Control Protocol), UDP(User Datagram Protocol)를 통해 임의적 접근통제(DAC: discretionary access control)와 강제적 접근통제(MAC: mandatory access control)[8]를 하여, 비인가자의 침입을 차단한다.

2.2 NAT(Network Address Translate)

방화벽의 특정한 네트워크 인터페이스 카드를 거쳐서 전송되는 패킷을 검사하여 지정된 IP와 목적 포트를 가지고 있는 경우에, 맵 테이블(Map Table)을 만들어 IP 주소를 변환 시킨다. 그러나 방화벽 외부망 사용자의 방화벽 내부 호스트로의 접근 시에는, 맵 테이블이 존재하지 않으므로 방화벽의 내부망에 접근 할 수 없다.

2.3 프락시(proxy) 및 인증(Authentication)

사용자가 접속하는 프락시에 대한 모든 접속에 대한 사용자에 대한 인증, 보안관리자에 대한 인증 및 사용자 그룹에 대한 인증과 사용자의 접속포트와 제한시간을 적용할 접근통제규칙 및 접속에 대한 Telnet, FTP, HTTP, SMTP, PoP3, Rlogin, 네트워크 그룹 등 특정 프로토콜을 위한 프락시서버가 작동하여, 프락시서버의 보안기능에 의해 접근 및 허용을 결정한다.

2.4. 무결성(Integrity) 및 전송무결성(VPN)

방화벽 내에 무결성기능은 선택한 영역에 대한, 추가, 수정 삭제 등이 발생 하였는가를 체크 하여 위반한 사항에 대해 보안 관리자에게 통보한다. VPN 기능은 전송 중 IPSec 과 IKE 표준[9]을 적용 하여 데이터의 변조 및 손실에 따르는 4가지 형태로 보안성을 제공하며[10], 어플리케이션[11]에서도 무결성, 비밀성, 송신자 인증기능을 제공하여 사용자에게 투명한 정보전송을 제공한다. 최근 VPN은 정보보호제품의 한 항목으로 분리해서 인증을 받게 될 것이다.

2.5 관리 및 감사(Auditing) 기록

침입차단시스템은 통과하는 모든 송수신 패킷에 대해 로그 파일(log file)을 기록 할 수 있다. 로그 파일에는 날짜, 사용시간, 사용자, 기록형태, 호스트(host), 서비스, 중요도, 사건형태 등을 기록하며, 이 기록을 토대로 한 감사기록 및 추적관리를 하며, 보안관리자에게 보안기능 과 정책을 수행할 수 있도록 하는 관리자메뉴가 있다.

2.6 암호화

방화벽에서의 내용에 대한 암호화와 함수는 정보보호 서비스의 하나로, 인증 시 패스워드에 관한 암호화 도구로는 S/Key 등이 있으며, 전송 내용에 대한 암호화는 RSA, 3DES, CAST, Bluefish, Twofish 등[12]이 있고, 무결성 체크에 대한 암호화는 MD5, SHA-1 등[12]을 사용한다.

Ⅲ. 무선방화벽의 설계

1. 설계 목표

■무선으로 접속된 외부와 내부 네트워크, 혹은 중요한 정보 전송의 유일한 경로(gateway)에 설치되어, 양자간에 오가는 모든 통신을 감시하여, 허용되지 않는 침입을 차단하여, 이로써 불법적인 네트워크 침입으로부터 내부 네트워크 시스템들과 중요한 정

보자원의 호스트들을 보호한다.

■방화벽의 기본 기능인 패킷필터링과 NAT 및 인증 그리고 감사기록 및 암호화 기능들이 무선방화벽에서 이루어 지도록 한다.

■무선에서의 이동 단말기 사용이 투명성있게 보장되도록 한다.

2. 설계 환경

아래 그림 2와 같이 이동단말기 사용자들과 무선환경을 통하여 내부 정보자원에 접속 할때에 반드시 게이트웨이로 설정된 무선방화벽을 거치도록 설계한다.

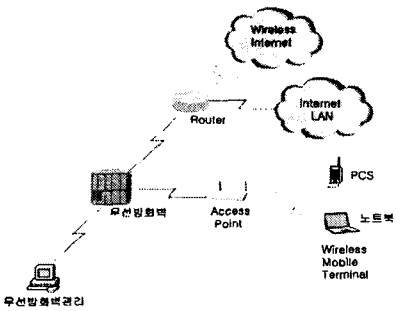

그림 2. 무선방화벽 설치 환경
Fig. 2. Wireless Firewall Install environment

3. 기능 설계

무선방화벽의 기능을 구현하기 위해 국가에서 인증하는 방화벽의 중요 기능들이 작동[13]되도록 설계한다.

3.1 패킷필터링(Packet Filtering)

무선방화벽은 억세스 포인터를 통한 무선 접속이나, 외부의 무선망에서 접속시 라우터를 통해 접속시에 사용자들이 공인받는 내부 정보서버로의 접근을 위하여 그들 자신을 인증할 때 동적으로 패킷필터링을 하도록 그림 3과 같이 한다.

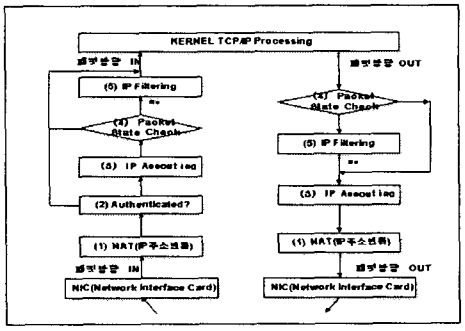

그림 3. 패킷필터링에 의한 패킷 흐름도
Fig. 3. Packet flow in Packet Filtering

3.2 NAT(Network Address Translate)

주소변환시에는 IPv4 체제에서는 IP 부족에 따른 내부의 사설 주소를 확보하고, 외부에서 내부보안을 위한 커튼메커니즘을 구성한다. 그리고 확장될 IPv6 체제에서는 맵테이블을 이용하도록 내부 보안을 구성한다.

3.3 인증(Authentication)

개인의 이동단말을 사용하여 접속을 할 시 CA로부터 사용자에 대한 인증을 받도록 한다. 그림 4에서 사용자 인증을 받는 과정을 나타냈다.

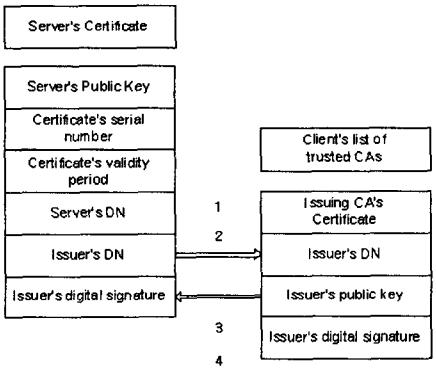

그림 4. 사용자 인증
Fig. 4. user authentication

3.4. 무결성(Integrity) 및 전송무결성(VPN)

방화벽 내부의 중요자료에 대한 주기적 무결성을 체크하도록 하고, 외부의 다른 네트워크와의 인터넷 공중망으로 연결된 환경에서의 정보전달에 대한 보안이 이루어지도록 다른 무선방화벽 들과 VPN을 수행할 수 있도록 한다. 무결성에 관한 프로세스를 그림 5에 나타냈다.

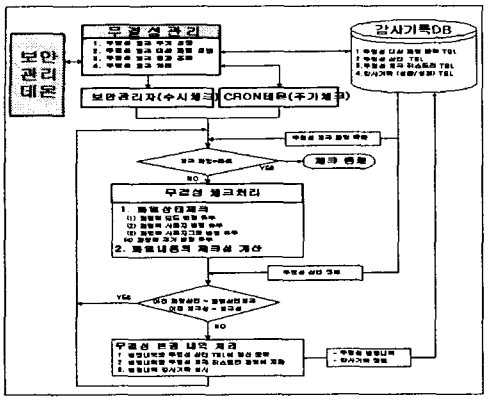

그림 5. 무결성 흐름도
Fig. 5. flow for Integrity

3.5 관리 및 감사(Auditing) 기록

무선방화벽을 통과하는 패킷에 대하여 모든 이벤트 별로 기록을 저장하도록 설계하였다. 표 1은 감사기록 설계에 관한 내용이다.

표 1. 감사기록 설계표
Table 1. design of Auditing

입력 항목	입력변수 이름	최소길이(값)	최대 길이(값)
시작년월일	s_ymd	8	8
종료년월일	e_ymd	8	8
사용자ID	userid	6	8
기록형태별	type	combo box	combo box
출발지 주소	subject	32	32
목적지 주소	object	32	32
서비스별	servicetype	combo box	combo box
중요도별	grade1~grade4	check box	check box
사건형태	rectype	combo box	combo box
원격기록조회	remoteaddr	64	64

Ⅳ. 무선방화벽의 구현 및 검증

1. 구현

■하드웨어: 서버급 400MHz의 1CPU와 512M의 MM, 32G의 HDD, 10/100BASE-T Ethernet 3 포트의 시스템을 구현[14]하였다.

■소프트웨어는 DHCPv3와 OpenBSD의 IPF 그리고, OpenSSH 등[15]을 이용하였다.

1.1. 패킷필터링

무선방화벽은 엑세스 포인터나 외부 무선망을 이용한 라우터를 통해 사용자들이 접근할 때 사용자를 인증하며, 동적으로 패킷필터링을 위해 DHCP[16] (Dynamic Host Configuration Protocol)서버를 이용한다. DNS나 ICMP와 같은 접근은 허용한다. 사용자가 웹서버에 이어질때는, 그들의 IP 주소는 기록되고, 로그가 성공하면 무선방화벽 필터리스트를 통해 기록된다.

1.2. NAT

실험실의 IPv4환경에서 나타낸 NAT 화면이 그림 6이다.

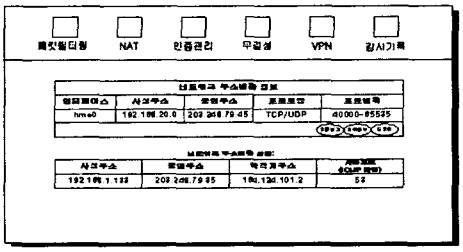

그림 6. NAT화면
Fig. 6. display of NAT

1.3 프락시 및 인증

웹을 통해 들어오는 인증정보는 SSL(Secure Socket Layer) 에서 RSA 암호화를 통해 자체 구축한 CA 서버로부터 사용자의 암호화된 인증서를 부여받아 접속에 성공하였다. 그림 7은 사용자에 대한 인증절차를 나타낸 것이다.

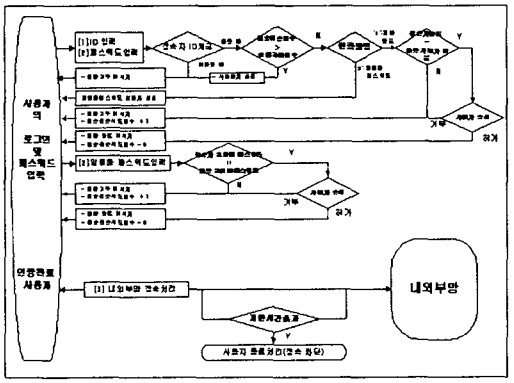

그림 7. 사용자에 대한 인증 흐름도
Fig. 7. flow of user Authentication

1.4 무결성 및 전송무결성

소프트웨어를 통한 암호화를 통해 무결성을 확보하였으며, 또한 전송구간에서도 전송무결성을 확보 하였다.

1.5 관리 및 감사 기록

DHCP 서버는 어떤 MAC 주소가 IP 어드레스를 요청하느냐 하는 기록을 유지하며, 이벤트가 발생 시마다 확인하여 syslog에 저장한다. 그림 8은 로그가 표시되는 화면이다.

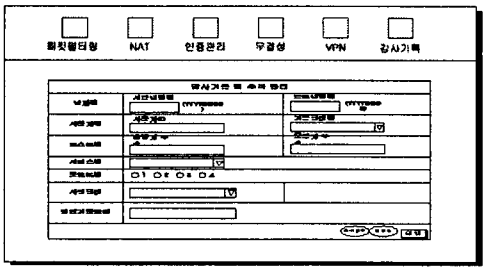

그림 8. 감사기록 화면
Fig. 8. display of Auditing

2. 검증

노트북에서 해킹프로그램인 DoS(denial of Service) 공격을 5회 실시 하였고, 그 외 ICMP flood, UDP flood, ping of death, IP spoofing, land attack 등으로 각각 5회씩 공격을 하였으나 무선방화벽을 침입하지 못했다.

그리고, NAT와 함께 무선방화벽 내부 PC에 사설주소를 부여하고 나서 외부 인터넷 서비스를 실험한 결과 정상적인 작동과 외부에 커튼 메커니즘이 이룩 되었음을 확인하였고, 무선 노트 북에서 실시한 인증부분도 자체 CA를 통해 인증되어 정상적인 로그 승인이 되었다.

소프트웨어를 통한 암호화 부분에서도 중요자료 검증을 한 결과 변경된 자료가 없이 무결성을 확보 하였으며, 통과된 패킷에 대한 시간별 사용자별, 서비스별 감사기록이 남는 것을 확인하였다.

V. 결론

본 논문에서는 한국에서의 무선 방화벽의 필요성을 강조하였고, 방화벽의 보안성이 검증된 국가 인증방화벽의 내용 및 방화벽의 목적과 기능을 파악하여, 이를 무선상태에서 적용할 수 있도록 하였다. 이를 위하여 무선방화벽의 개념을 확정짓고, 그리고 무선 방화벽의 목적과 기능에 맞게 설계를 하였고, 이를 토대로 실험실 환경에서 구현을 하여 무선방화벽의 패킷필터링과 NAT 및 인증 그리고, 감사기록관리 기능을 구현하여, 테스트 한 결과 방화벽의 위 기능들이 작동됨을 확인 하였다.

향후 연구과제로 무선방화벽을 상용화시키고, 세계 시장에서 경쟁력을 갖추려면, 현재 사용한 암호화 알고리즘 대신에 이동환경에 더욱 비도가 높으며, 비트수가 적어 이동 환경에서 효율적인 ECC와 IPsec 등의 알고리즘을 통한 암호화 방법을 도입하고, 무선도 IEEE 802.11b에서 IEEE 802.11a까지 확대하여 무선기지국의 사용범위와 게이트웨이의 용량을 확장하는데 더욱 연구하여야 하며, 세계 전자상거래에서 인증되고 있는 PKI 인증회사와의 무선 연동을 통한 사용자 인증부분을 확대하는 것을 연구개발 하여야 할 것이다. 이러한 무선방화벽에 대한 연구개발을 통하여 세계시장에서도 우수한 기술력과 경쟁력을 갖춘 정보보호기술과 제품이 되리라고 확신한다.

참고문헌

[1] 한국인터넷정보센터, 2002년12월 인터넷통계월보, KRNIC, p2, 2003.1

[2] 박대우,전문석, K4 방화벽의 CPU 및 보안규칙의 증가에 따르는 성능평가연구, 한국전자거래학회, 2002.12

[3] 정보통신부고시, http://www.mic.go.kr/, 정보

보호 시스템 평가 인증지침, 정보통신부, 2002.8
[4] 정보통신부고시, http://www.nis.go.kr/, 정보보호 시스템 공통평가 기준, 정보통신부, 2002.8
[5] 정보통신부고시, 정보통신망 침입차단시스템 평가기준, 정보통신부, p 1-2, 2002.2
[6] 김재헌, 조자영, K4E 방화벽의 보안기술, 정보처리 학회지, 제9권 제1호, 2001.1
[7] 정보보호시스템인증제품, 평가인증제품현황, http://www.nis.go.kr/kr/security/info119/product .html , 국가정보원 , 2003.2
[8] 김재성, 홍기웅, 김학범, 심주걸, 침입차단시스템을 위한 강제적 접근통제법설계, 한국정보처리학회, 제 5 권 제4호, 1998.4.
[9] http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-05.txt.
[10] ISTF-003, Implementation Technology for secu re VPN in IP Layers, 인터넷보안기술포럼, 2001. 5.
[11] 최준호, 김판구, 네트워크상에서의 바이러스 차단을 위한 방화벽시스템의 설계 및 구현, 정보처리학회 논문지 C 제8-C권4호,
[12] 2001.8한국정보보호진흥원, 정보보호개론, 교우사, p17-42, 2000.7.
[13] 전문석, 박대우, 매직캐슬 V1.0, 매직캐슬 V3.0, 국가정보원, KISA, 2001.4.18, 2003,3 한국정보보호진흥원, http://www.kisa.or.kr/, 평가체계, 시험평가, 평가인증제품현황, 2003.3.
[14] http://www.netgear.com/products/ details/FM114P.asp?view=, 2003.2
[15] http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless , 2003.2
[16] http://www.ietf.org/rfc/rfc2131.txt, March 1997

저 자 소 개

박 대 우

1987년 2월: 서울시립대학교 경영학과 졸업 (학사)
1995년 2월 : 숭실대학교 컴퓨터학부 (전산부전공)
1998년 8월 : 숭실대학교 컴퓨터학과 (석사)
2001년 8월 : 숭실대학교 컴퓨터학과 (박사수료)
1987년 8월 : 동구여상 정보처리,정보통신과 교사
2000년 2월 : Entrust-Korea 연구소 부소장
2000년 10월 : 매직캐슬정보통신 부사장/연구소장
2003년 3월 : 숭실대학교 대학원 겸임교수
관심분야 : 정보보안, 네트워크, 이동통신, 무선방화벽, IMT-2000보안, 위성통신보안, Cyber Reality