韓國 컴퓨터情報學會 論文誌
第8卷 第1號, 2003. 3.

2003-8-1-1-5

32비트와 64비트 K4 방화벽 성능 비교에 관한 연구

박 대 우* 정 우 식**

The study of performance evaluation between 32bit and 64bit K4 Firewall System

Dae-woo Park* Woo-sik Jung**

요 약

현재 국가에서 K4 방화벽(Firewall)에 대해 보안성을 인증하고 있으며, 인증을 받은 방화벽이 공공기관에서 사용되고 있다. 본 논문에서는, 이 방화벽의 인증체계 및 기능에 대해 분석한다. K4 방화벽 중 한국에서 범용적으로 사용되는 Solaris를 운영체제로 하는 32비트 방화벽에 비해, 64비트 방화벽의 달라진 내용을 분석하고, 기존 32비트 체제 방화벽성능에 비해 최근 인증을 받고 있는 64비트 체제의 Solaris 방화벽을 비교 평가하여, 32비트에 비해 64비트 방화벽이 2배 이상 성능 개선이 나타남을 비교 평가한다. 그리고, 결론에서 K4 방화벽 및 대한민국 방화벽의 연구 및 개발에 방향을 제시하여 세계에서 경쟁력있는 시스템으로 도움이 되고자 한다.

Abstract

Korea has been issued on K4 Firewall Certificates for security, and these K4 Firewalls has been installing all Korean public organizer. In this paper, I would analysis process and functions of K4 Firewall. I had been created by difference and performance test between existing 32bit and latest 64bit K4 Firewall System on Solaris Operating System that wide use in Korea, So that the result of improved more two times passed rate on 64bit than 32bit on Solaris K4 Firewall System, At finally, I would conclude that the change direction will be useful for research and development on K4 Firewall System and Korean Firewall System which is a very competitive system in the world.

* 숭실대학교 컴퓨터학과 통신연구실
** 동서울대학 소프트웨어과

접수일자 : 2003. 1.15
심사완료 : 2003. 3. 5

Ⅰ. 서론

국내 인터넷 사용자는 2002년 12월 2,627만명에 이르고, kr 도메인도 2001년 457,450개에 비해 515,200개로 12.62%가 증가[1]되었다. 하지만 인터넷 사용자 증가에 따른 정보화의 역기능으로 인한 정보보호 침해사고도 매년 증가하여, CERTCC-KR에 접수된 국내 침해사고도 2002년에 15,192건에 이르러 2001년 5,333건에 비해 약3배의 증가[2]를 보이고 있다. 이와 같이 정보보호 침해사고는 불법적으로 정보를 취득하여 해를 주거나, 네트워크의 시스템을 손상하거나, 네트워크 시스템에 장애를 유발하는 것이며, 정보보호 목적 중에 하나가 이들 사고로부터 정보자원을 안전하게 지키는 것이다.

정보보호 목적을 달성하기 위한 대표적인 정보보호시스템 중의 하나가 방화벽시스템 이다. 방화벽시스템은 외부와 방화벽 내부 네트워크의 연결하는 유일한 경로(gateway)나, 혹은 중요한 정보전송의 유일한 전송로에 설치되어, 방화벽시스템을 통과하는 통신 및 서비스를 감시하며, 허가 또는 인증되지 않거나 비정상적인 사용자가 침입하는 것을 차단할 수 있다.

본 논문에서는 현재 국가에서 보안성을 평가하고 인증하고 있는 방화벽에 대한 인증기준과 인증방화벽에 대한 기능을 분석하고, 국가에서 보안성이 검증된 K4등급 인증평가를 받은 방화벽[3] 중, 32 비트의 방화벽에 비해 64비트의 방화벽이 얼마만큼의 성능 개선이 이루어져 있는가에 대한 내용분석과 성능비교를 평가 연구하여, 이를 토대로 한 방화벽성능개선 효율성을 측정하여 앞으로 연구개발될 우리나라 방화벽의 성능개선에 도움이 되는 방향을 제시 하고자 한다.

Ⅱ. 관련연구

1. 방화벽 인증체계

한국에서의 방화벽은 제품명으로는침입차단시스템이며, 이러한 정보보호제품으로써 국가에서 보안성을 보증하기 위해 정부차원의 인증을 국가정보원에서 시행하고 있으며, 현재 2002년 8월 5일 정보보호시스템평가인증지침(정보통신부고시 제2002-41호)으로 개정되었다.[4]

침입차단시스템 평가기준은 보안기능의 신뢰성을 확인하기 위한 보증요구 사항으로 개발과정, 시험, 형상관리, 운영환경, 설명서, 취약성의 6가지 사항으로 이루어진다. 평가등급은 K1 등급을 최저단계로 하고, K2, K3, K4, K5, K6 그리고 K7를 최고 단계로 하여 총 7단계로 구분하는데, 국가 및 관련 공공기관에 설치 하기위한 방화벽은 일반적으로 K4등급 이상의 인증을 받은 방화벽을 채택하고 있다. 국가정보원에서는 향후 국제표준의 ISO/IEC 15408-1의 원본인 국제공통평가기준[5]을 국내 표준으로 제정하고 정보보호제품의 공통평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7의 7개의 등급으로 구분된다.[6]

현재 인증받고 있는 K4인증 침입차단시스템의 일반적인 모델은 그림 1과 같이 하이브리드 듀얼 홈드게이트웨이 방식(Hybrid Dual-Homed Gateway)에다가 상태정밀검사방식(Stateful Inspection)[7]을 도입하여 사용하고 있다.

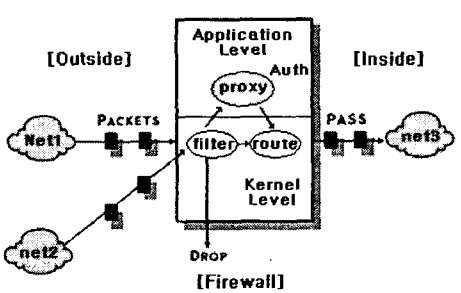

그림 1. 하이브리드 듀얼 홈드게이트웨어 방식
Fig. 1. Hybrid Dual-Homed Gateway

2. K4 방화벽 기능

정부에서 보안성이 검증된 K4인증 방화벽의 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. VPN기능은 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.

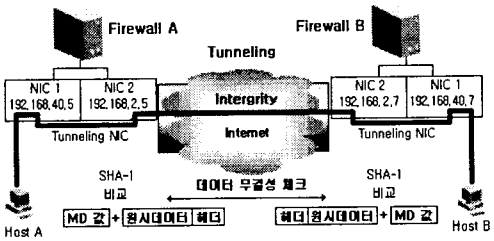

그림 2. 방화벽 VPN을 통한 전송 무결성
Fig 2. Firewall VPN intergrity through Internet

2.5. 관리 및 감사(Auditing) 기록

침입차단시스템은 통과하는 모든 송수신패킷에 대해 로그 파일(log file)을 기록 할 수 있다. 이 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.

3. K4 인증 방화벽의 운영체제

K4 방화벽의 기능평가는 한국정보보호진흥원(KISA)에서 담당하고 있다. 아래의 표 1과 같이 2003년 1월에 평가 인증 후거나, 평가인증 중인 K4 인증 등급이상의 침입차단시스템의 운영체제는 UNIX 계열의 Solaris와 X86, IBM- AIX, HP-UX 그리고, Windows 계열의 NT, Windows2000, XP 등이 있다.[12]

현재 한국에서 범용적으로 사용되는 침입차단시스템의 운영체제인 UNIX 계열의 Solaris K4 방화벽은 32비트 체제와 64비트 체제로 나누어 볼 수 있다. 즉, Solaris 2.5.1 과 Solaris 2.6, Solaris 7 까지를 32 비트 체제로 분류해 볼 수 있고, Solaris 8부터는 64 비트체제로 분류해 볼 수 있다. 위의 분류에서 Solaris 7을 32비트 체제와 64비트 체제로 혼용 작동 시킬 수 있다고는 하나, 성능면에서의 정확성을 위해 Solaris 7을 성능 실험 비교 대상에서 제외하였다.

표 1. Solaris K4 방화벽 및 운영체제
Table 1. SolarisK4 Firewall & Operating System

K4인증	평가 제품명 및 버전	운영 체제
평가완료	SecureShield Firewall V1.0	Solaris 2.5.1
	인터가드 V1.5	Solaris 2.5.1
	수호신 V2.0	Solaris 2.5.1
	SecureWorks V2.0	Solaris 7 for x86
	SecureWorks V2.0	Solaris 7
	수호신 V3.0	Solaris 7 for x86
	매직캐슬 V1.0	Solaris 2.5.1
	수호신 V3.0	Solaris 7
	SecureWorks V3.0	Solaris 8 for x86
	SecureWorks V3.0	Solaris 8
평가진행	MagicCastle V3.0	Solaris 8
	FzoneWall Plus V1.0	Solaris 8 for x86

4. K4 방화벽의 32 비트와 64 비트 차이점

현재 K4인증 방화벽 중 운영체제가 Solaris인 방화벽은, 하드웨어에다 32비트 운영체제나 64비트 운영체제를 인스톨하고, 그 위에 방화벽 소프트웨어가 설치되어 방화벽 단독기능만을 수행하는 정보보호시스템으로 운용되고 있다. 여기에서 성능 분석대상이 되는 Solaris 운영체제는 32비트 체제에서 64비트 체제로 발전하면서, 크게 다음과 같은 3가지 차이점을 개선 하였다.

첫째는 확장된 정밀도(Extended Precision)

둘째는 확대된 데이터 집합체 지원

(Large Dataset Support)

셋째는 큰 가상주소 공간

(Large Virtual Address Space) 이다.[13] 즉 기존 32비트 운영체제에 비해 정수 연산 성능과 실수 연산 처리가 64비트로 처리하면서 수학계산의 정밀성이 확장되었고, 64비트의 비동기적 입출력을 지원하며, 1테라 바이트(Terabyte)로 확대된 데이터 집합체를 지원하고, 32비트 운영체제에서 부족한 메인메모리를 위하여, 직접 물리적인 가상적 메모리를 확대하여 사용할 수 있기 때문에 32비트 운영체제 보다 향상된 기능의 운영체제를 구축할 수 있다.

지금까지, K4방화벽 소프트웨어 개발에서, 절차적(procedural) 언어로 구현되어있는 구조적 기법에 의한 프로그램의 수행은, 함수나 서브 프로그램 단위로 순차적이면서 지역성을 잃지 않고 진행된 경우가 보통이었다. 이 경우에 반복적으로 참조되는 성질을 이용한 메모리 캐시의 적중률이 높아져 효율적이었다. 그러나 객체 지향 기법에서의 프로그램은 평면적, 병렬적으로 수행되는 성질이 강하여 페이지 폴트(page fault)의 빈도가 높아지고, 이는 페이지 교체와 메모리 캐시의 실패율 증가로 연결되어 CPU의 성능을 낮추는 결과를 가져온다. 이때 32비트 프로세서가 2단계 페이징(paging)을 갖는다면, 64비트 프로세서는 3단계 페이징 능력을 갖는다.[14] 따라서, 이론적으로 18exebytes까지 메모리의 확장이 가능한 64비트 프로세서는 요구 페이징의 부하를 현격하게 감소시킬 수 있어, 충분한 메모리의 활용과 CPU성능의 개선 효과가 64비트 방화벽 소프트웨어에 성능개선 효과를 제공하는 것이다. 아래의 표 2에서 Solaris 각 플랫폼(Platform)에 의한 하드웨어 MMU(Management Memory Unit)에서의 HAT(Hard Address Translation)단계 수행 능력을 보여주고 있다.[15]

표 2. Solaris 메모리관리장치에서의 HAT 수행능력
Table 2. Solaris MMU HAT implementations

Platform	No. of Contexts	Size of TLB	TLB Fill	Virtual Bits	Physical Bits
SPARC 1,2	8	64	Hardware	32	32
Micro SPARC	65536	64	Hardware	32	32
Super SPARC	65536	64	Hardware	32	36
Ultra SPARC I,II	8192	64 x 2	Software	44	41
Intel Pentium			Hardware	32	36

여기에서 64비트 체제의 Ultra SPARC I, II가 다른 플랫폼에 비해 TLB(Translation Lookaside Buffer)에서 2배의 크기를 가지고, 44비트의 가상주소와 41비트의 실제주소를 사용하여 성능을 개선 시킨 것으로 나타난다. 여기에서 Solaris K4 64비트 방화벽은 32비트 메모리 어드레싱(Memory Addressing)을 64비트 메모리 어드레싱으로 활용하여 프로세서, 어플리케이션, 운영체제 등에서 메모리를 테라 바이트 수준까지 활용할 수 있는 능력을 가졌지만, 국내 방화벽 소프트웨어 개발은 64비트 어드레스 공간을 처리하지 못하고 있고, 실제 K4 64비트 방화벽에서의 각 기능에 대한 소프트웨어적인 모듈단위의 활용도에 대한 64비트 처리 체제로의 완전한 전환은 아직 이루어 지지 않고 있다.

Ⅲ. 32 비트 체제와 64비트 체제의 성능비교

1. 성능 평가 장비 및 프로그램 구성

K4 방화벽 시스템 평가에 사용되는 하드웨어는 SUN Ultra 80에 1CPU와 메인 메모리 1024Mbyte, 32Giga 하드디스크에 32비트 운영체제로 Solaris 2.5.1을 설정하고, 64비트 운영체제로 Solaris 8을 설치하고, 각각에 K4인증을 받은 침입차단시스템 소프트웨어를 설치하여 가동하고, 방화벽의 기능에 이상이 없는지를 실험한 후, 운영체제에 따른 비교평가에서는 32비트와 64비트를 차례로 설치 성능평가를 한 후 값을 비교 하였다. 성능평가는 방화벽 성능평가 장비인 Smart비트-2000에서 패킷생성 툴(Tool)인 Smart TCP 이용하여 네트웍 트래픽(Network Traffic)을 발생시켰고, 성능 측정 프로그램은 Smart Applicat을 이용하여, TCP Flow를 발생시켜서 성능실험을 하였다.

성능 실험을 위한 방화벽 성능 실험에 대한 배치는 현장마다 다르나, 기본 형태의 현장배치는 그림 3과 같이 되어있다.

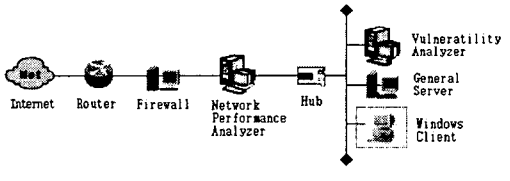

그림 3. 방화벽 성능실험 배치도
Fig. 3. firewall test arrangement

2. 성능 평가 조건 및 방법

성능 평가를 위한 실험조건으로 전송부하에 대한 성능실험을 하였고, 방화벽에 대한 기본 보안 정책은 다음과 같다.

■Any_in(내부) --- Any anyTCP, anyUDP, Ping 허용

■Any(외부) --- Any_in anyTCP, anyUDP, Ping 허용

방화벽 성능 실험을 하기 위해 40군데 이상의현장에 대한 보안규칙 설정을 조사한 바, 각각의 내부시스템과 조직의 특성상 보안규칙 설정의 방법 및 보안규칙 설정의 개수와 규칙 종류도 다양 하였으나, 평균 50개 미만이 대부분인 것을 감안하여 50개로 기준을 설정하였다. 각 보안규칙의 설정내용은 현 실무에서의 적용규칙을 그대로 적용하고, 현장의 보안관리자 의견을 최대한 반영한 후 성능실험을 하였다.

32비트와 64비트의 운영체제별 성능평가 실험에서는 K4 방화벽의 기능 중, 패킷필터링과 NAT, 프락시 및 인증서비스 기능을 모두 적용한 후, 패킷의 프레임 사이즈(Frame Size) 별로 패킷손실율을 측정 하는 성능실험을 하였다. 즉 성능실험장치를 통해 128byte, 256byte, 512byte, 1024byte, 1280byte, 1518byte의 프레임 사이즈를 가진 전송부하를 100Mbyte로 생성하여 네트워크 트래픽(Network Traffic)을 발생시키고, 이를 32비트와 64비트의 각각 K4방화벽에 대하여 한 방향 전송을 시행하고, 이를 5회 반복하여 패킷전송율(Pass rate)을 산출한 후 평균 값을 계산하여 네트워크 처리율(Passed Rate)을 비교하였다. 실험 조건은 표 3과 같다.

표 3. 네트워크 처리율 실험조건
Table 3. test condition of Passed Rate

item	value
Test Duration	120 sec
Minimum Frame Size	128 byte
Maximum Frame Size	1518 byte
Initial Rate	30 %

Ⅳ. 32비트와 64비트 성능평가

우선 하드웨어에 32비트와 64비트의 운영체제만을 설치하여 성능실험을 하였다. 방화벽 설치전과 설치 후의 성능 실험의 결과 그림 4와 같이 128byte 한 방향 초당 트래픽 전송율은 32비트는 70.31%, 64비트에서는 97.69%의 차이를 보였다. 256byte 성능측정 에서는 초당 트래

픽 전송율은 32비트는 87.62%, 64비트에서는 98.75%의 차이를 보였다. 그러나 512 byte 이상 에서는 99.81% 이상을 보여 하드웨어에 운영체제만 인스톨 시에 성능차이는 작게 나타났다.

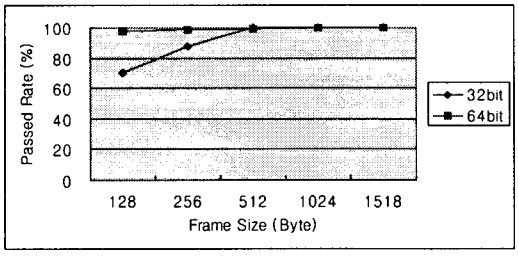

그림 4. 방화벽소프트 설치 전 32비트와 64비트성능 비교
Fig 4. performance 32bit vs 64 bit before install firewall s/w

K4 방화벽 시스템을 구축 후에 K4방화벽 기능을 적용한 후의 성능평가 실험에서는 위 그림 5와 같이 32비트의 방화벽에서 성능 실험 결과는, 128byte에서 4.37%, 256byte에서 12.50%, 512byte에서는 19.37%, 1024byte에서는 25.61%, 1518byte에서는 27.49%의 네트워크 처리율을 보였으며, 64비트의 방화벽에서는 128byte에서30.67%, 256byte에서 56.97% 의 네트워크 처리율을 보였으며, 512byte이상의 패킷 크기에서는 패킷손실율이 적은 네트워크 처리율이 측정되었다.

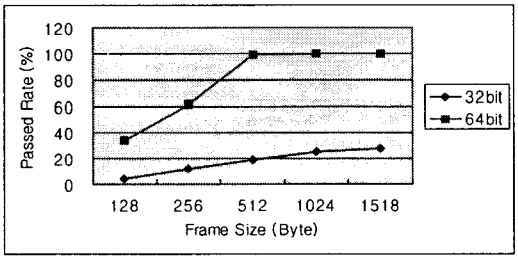

그림 5. 32비트와 64비트 방화벽 성능 비교
Fig. 5. performance 32bit vs 64bit of firewall

V. 결론

본 논문에서 확인된대로 32비트 K4방화벽에 비해 64비트 K4방화벽이 파일처리의 효율성이나, 메모리의 확장 그리고, 운영체제의 효율성으로 인하여, 방화벽의 단점인 패킷의 처리효율을 향상시킨 것으로 나타났다. 특히 32비트와 64비트의 K4방화벽의 성능비교 실험의 결과에서 산출된 평균 값을 비교한 결과, 64비트 방화벽이 네트웍처리율에서 두배 이상의 성능개선 효과가 있었음을 밝혀 내었다.

방화벽이 소프트웨어와 운영체제 및 하드웨어로 이루어진 하나의 시스템이란 점에서 64비트 방화벽의 성능개선이 이루어진 기능 및 내용별 비교 결과의 분석은 차후에 더욱 확장되어 연구 되어져야 하겠지만, 당분간 국가정보원의 K4인증을 받은 64비트 체제의 방화벽이 주류로 사용되어질 것으로 여겨진다.

따라서 차후 인증되는 방화벽의 보호서비스 및 보안기능을 연구 개발 시에는, 64비트 체제의 CPU 프로세서와 메모리 및 운영체제를 활용하여, 다중 패킷을 동시에 처리 할 수 있는 방법들이 연구 개발 되어져야 한다. 더욱이 급속한 초고속 인터넷환경으로의 변환과, 멀티미디어 데이터의 전송에 따른 통신량의 급격한 증가로 인한 대용량 트래픽을 감안할 때 기가비트(Gigabit) 방화벽에 대한 연구 및 개발이 시급해 보이며, 특히 방화벽시스템의 내부에서도 하드웨어 및 운영체제와 통합되어 전용방화벽으로써의 성능 향상을 이룰 수 있어야 하겠다.

참고문헌

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

[2] CERTCC-KR통계, http://www.certcc .or.kr/, 2002. 11.

[3] 정보보호시스템인증제품, 평가인증 제품 현황, http://www.nis.go.kr/kr/security/info119/product.html, 국가정보원 , 2003.2

[4] 정보통신부고시, http://www.mic.go.kr/, 정보보호시스템평가인증지침, 정보통신부, 2002.8

[5] 정보통신부고시, 정보통신망 침입차단시스템 평가기준, 정보통신부, p 1-2, 2002.2

[6] 정보통신부고시, http://www.nis.go.kr/, 정보보호시스템 공통평가기준, 정보통신부, 2002.8
[7] 김재헌, 조자영, K4E 방화벽의 보안기술, 정보처리 제9권 제1호, 2001.1
[8] 김재성, 홍기융, 김학범, 심주걸, 침입차단 시스템을 위한 강제적 접근통제법설계, 한국정보처리학회, 제5 권 제4호, 1998.4.
[9] http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-05.txt. 2003.2
[10] ISTF-003, Implementation Technology for secure VPN in IP Layers, 인터넷보안기술 포럼, 2001. 5.
[11] 최준호, 김판구, 네트워크상에서의 바이러스 차단을 위한 방화벽시스템의 설계 및 구현, 정보처리학회 논문지 C 제8-C권4호, 2001.8
[12] 한국정보보호진흥원, http://www.kisa.or.kr 평가체계, 시험평가, 평가인증제품현황, 2003.2.
[13] Sun Microsystems, http://wwws.sun.com/software/solaris/faqs/64bit.html#0q0, 2002.11
[14] Daniel P, Bovet, Marco Cesati, Understanding the Linux Kernel, O'Really & Associates, p45-51, January 2001.
[15] Jim Mauro, Richard MacDougall, SOLARIS Internals, Sun Microsystems Press, p190-194, 2001

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, 무선 방화벽, IMT-2000보안, 위성통신보안, Cyber Reality,

정 우 식

1980년 광운대학교 전산학과 졸
1982년 숭실대학원 전산학과 졸
1982 - 1984 한국전력공사 전자계산소 근무
1984.3 - 현재 동서울대학 소프트웨어과 교수
1997 - 현재 숭실대학교 전자계산전공 박사 수료

관심분야 :
Network security, Software Engeering, Language 일반