論文
4-4-22

가상 사설망에서 프로토콜의 성능분석에 관한 연구
(A Study on Performance analysis of protocol in VPN)

김 도 문(Do-moon Kim)[1] 전 문 석(Mun-seok Jun)[2]

요 약

가상 사설망에 계층간에 사용하는 프로토콜이 각기 다르다. 네트워크 상에서 정보의 상호 교환은 기밀성과 무결성의 확보가 중요하다. 그러나 보안 방식에 따른 여러 형태의 장비들에 따른 프로토콜의 다양화로 인해 호환성과 가용성에 따르는 문제점이 있다. 그래서 정보의 암호화와 인증을 통해서 전송이 이루어진다면 제 3자의 공격으로부터 안전할 수 있다. 그러므로 가상사설망(VPN) 시스템 통한 터널링을 통해서 계층간 상호교환의 전송이 이루어진다. 본 논문에서는 인증된 공개키를 사용하여 계층2와 계층3에서 사용되는 각각의 프로토콜로서 정보가 전송될 경우 계층간의 성능분석 차이점을 파악하여 본다.

ABSTRACT

We are view of the information on VPN(Virtual private Network) into each difference layer protocol. network on mutuality exchanged of information is importance of the confidentiality and integrity. But it is presented problems about compatability and availability between variable equipment as several protocol. hence, it was achieved of the transmission through encryption and authentication of information, although there is secured an intended attack from the third intruder. so tunneling VPN system on achieving, each layer position transmit of mutuality exchanged.

This study will investigate the codification and certified security status when layer2 and layer 3 informations are each transmitted using protocol with integrity Public Key. In addition, we will using protocol and the performance analysis difference between layer2 and layer3.

1. 서론

컴퓨터와 네트워크 기술발달로 인하여 정보의 전달이 고속으로 전달되고 있다. 정보에 대한 신뢰성과 기밀성의 중요성이 인식이 더욱 절실히 느끼고 있다. 이러한 문제를 해결하기 위한 대처방안으로 공중 데이터 통신망인 인터넷을 통해서 전용선으로 활용할 수 있는 기술이 발전하고 있다. 가상사설망(Virtual private Network)이 이에 해당한다. 그러나 이 방법도 상존하는 취약점으로 인해 날로 심각해지는 해킹으로부터 안전하지 못하며, 취약점을 개선한 보다 안전하고 향상된 기

1) 정회원 : 동우대학 컴퓨터그래픽과 조교수
2) 정회원 : 숭실대학교 컴퓨터학부 정교수

논문심사 : 2003. 7. 4.
심사완료 : 2003. 7. 18.

능의 보안방법이 절실히 필요한 실정이다. 이에 본 논문에서는 PKI 기반하의 계층간의 프로토콜 설정을 통하여VPN 시스템 구현과 성능에 알아본다. 본 논문의 구성은 다음과 같다. 2장에서는 VPN의 개요에서 기존의 VPN이 갖는 보안상의 프로토콜을 기술하였으며, 3장에서는 본 논문에서 제안하는 가상사설망 구축에 따른 프로토콜과 PKI 인증 키에 대하여 알아보고 4장에서는 공개키를 이용한 VPN에 대한에 대한 계층간의 프르토콜의 성능을 비교분석하고 5장에서는 결론과 차후 연구방향 등을 기술한다.

2. 가상 사설망 (VPN, Virtual Private Network)

2.1 가상 사설망의 원리

공중 통신망에서 논리적인 회선을 마치 전용선에 의한 사설통신망처럼 사용하여 안전한 전송을 할 수 있도록 하는 것이다. 즉, 가상사설망(VPN)이란 기업이 공중망을 이용하여 경제적이고 안정적으로 통신망을 운영할 수 있도록 하는 솔루션을 의미한다[1]. VPN의 핵심 기술로서 사용되어지는 터널링 기술은 인터넷 상에서 외부의 영향을 받지 않는 가상적인 터널을 형성해 정보를 주고받도록 하는 기술로서, 시작지점에서 목표지점까지 상호 약속된 프로토콜로 세션을 구성하게 된다.

가상사설망은 인터넷과 같은 공중망을 이용하여 가상의 사설망을 구성하는 기술로 기존의 전용선을 이용한 사설망에 비해 저렴한 비용으로 외부와의 네트워크 정보 교환이 안전하게 구성할 수 있다는 면에서 각광을 받기 시작하였다. 가상사설망(VPN)은 상호 네트워킹 시나리오에 따라 통상 인트라넷 기반의 VPN, 엑스트라넷 기반의 VPN, 원격 접속 기반의 VPN이 있다. 구현 기술로는 터널링, 암호화 및 인증, 엑세스 제어로 구분할 수 있다. 그리고 불특정 다수의 인터넷 사용자에 대한 접근통제이고, VPN의 주요내용은 암호기술을 이용한 사설망을 인터넷으로부터 차단됨과 동시에 정보의 보안에 있다. 따라서 계층 2와 계층 3에서 VPN의 구축에 따른 보안 연계의 안전성이 있어야 한다.[3].

2.2 계층별 프로토콜

현재 가상사설망(VPN)에서 정의된 계층별 프로토콜은 〈표 1〉과 같다. 이 기종간의 네트워크 상에서 통신할 경우 각 계층별 프로토콜을 설정한 후 정보 전송이 가능하다. 제 2계층과 제 3계층의 프로토콜들은 각 역할의 차이점을 가지고 있다.

〈표 1〉 계층별 프로토콜
〈Table 1〉 Protocol of Layer

7 계층별 구분	지원되는 프로토콜
Application Layer Presentation Layer Session Layer Transport Layer	SOCKS V5, SSL
Network Layer	IPSec, VTP, ATMP
Data Link Layer	L2F, PPTP, L2TP
Physical Layer	

2.2.1 2계층 프로토콜

(1) L2TP(Layer2 Forwarding)

L2TP는 PPTP와 L2F를 결합한 방법으로서, IP/IPX 또는 NetBEUI 트래픽을 암호화하고 IP헤더로 캡슐화하여, 인터넷(X.25/FR) 또는 ATM을 경유하여 전송한다. L2TP는 터널(Tunnel)을 유지하기 위해 UDP와 일련의 L2TP 메시지(Message)를 사용한다. L2TP는 규격이 구체적이지 않아 구현물이 많지 않다는 단점이 있다. PPTP와 L2TP는 모두 데이터를 PPP로 캡슐화 하고 추가 헤더를 덧붙여 망으로 전송한다. 따라서 2개의 프로토콜은 매우 유사하지만 〈표 2〉와 같은 차이가 있다.

〈표 2〉 PPTP와 L2TP의 비교
〈Table 2〉 Comparison of PPTP and L2TP

구 분	PPTP	L2TP
지원 프로토콜	IP	IP,FR,X.25,ATM등
한 종점 사이에 지원되는 터널 수	한개	여러개
헤더 압축	지원하지 않음	지원함
터널 인증	지원하지 않음	지원함

(2) PPTP(Point-to-Point Tunneling Protocol)

PPTP는 마이크로소프트사가 개발한 방법으로서 IP/IPX 또는 NetBEUI Traffic을 암호화하고 IP헤더로 캡슐화 하여 인터넷을 경유하여 전송한다. PPTP는 Tunnel을 유지하기 위해 TCP연결을 사용한다.

첫째, Voluntary Tunneling은 PPP클라이언트가 ISP의 FEP(Front End Processor)와 PPP세션을 설정한다. FEP는 원격사용자가 모뎀이나 ISDN을 사용하여 액세스하는 라우터나 브릿지를 말한다.

FEP는 사용자로부터 RAS(Remote Access Server)로의 연결 요청을 받으면, RAS와 PPTP 세션을 열어 Client로부터의 모든 데이터를 PPTP를 통해 전송한다.

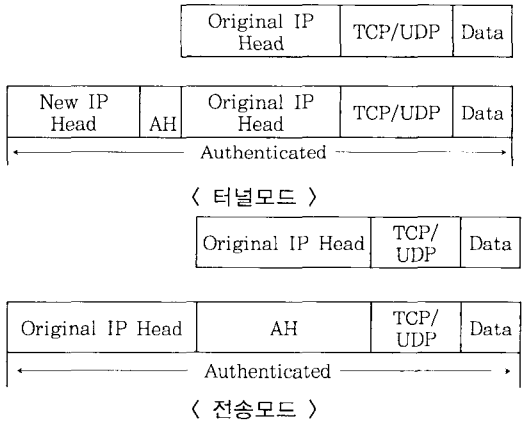
둘째, Compulsory Tunneling은 Client가 PPTP 기능을 가진 경우로서, 먼저 사용자가 FEP로 Dial Up하여 PPP세션을 설정한다. 그리고 나서 RAS와 PPTP 연결을 설정하기 위해 PPP세션과 함께 RAS로 다시 2번째 Dial Up을 수행한다. Client와 Server간의 데이터는 새로 생성된 PPTP 세션을 통해 전송된다.

2.2.2 3계층 프로토콜(IPSec)

IPsec은 트랜스포트 모드와 터널 모드 2가지가 있다. 트랜스포트 모드는 IP 페로이드(Payload)를 암호화하여 IP헤더로 캡슐화한다. 터널모드는 IP 패킷을 모두 암호화하여 인터넷으로 전송한다. IPsec은 AH(Authentication Header)와 ESP (Encapsulation Security Payload)의 두 가지 IP 헤더를 가진다.

(1) AH(Authentication Header)

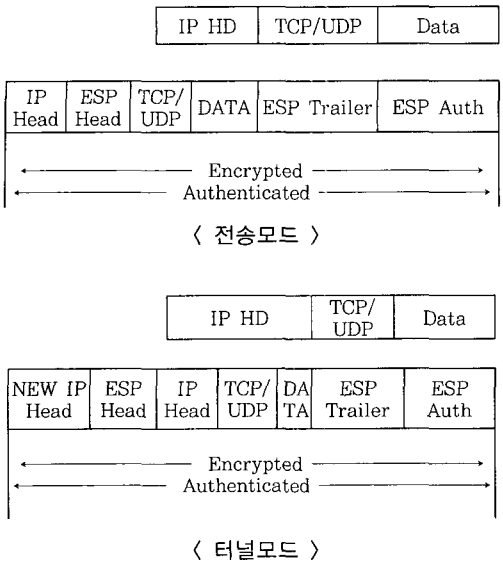
AH는 IP extension Header로서 IP 패킷(packet)에 대한 인증 여부를 제공한다. ESP와는 달리 AH는 전체 IP 패킷에 대한 인증 여부를 결정하게 된다. 터널모드 및 전송모드에서의 AH를 사용한 IPSec 데이터그램이다. 터널모드의 경우 AH는 IP 헤더와 페로이드 사이에 위치하여 전체 IP 패킷을 인증하며, 전송모드의 경우 새로운 IP 헤더와 AH가 앞부분에 첨가된다.



[그림 1] AH 헤더 구조
[Fig 1] AH header Architecture

(2) ESP (Encapsulating Security Protocol)

ESP는 다수의 보안 서비스를 제공하며, 기밀성, 발신인 인증, 데이터 무결성을 제공한다. 각각의 서비스들은 별도로 제공이 가능하다. 따라서 인증이 없는 기밀성 제공이 가능하다. 인증 데이터는 인증값으로 AH와는 달리 인증 서비스가 선택되었을 경우에만 존재한다. 기밀성 서비스가 선택된 경우 Payload data, Padding, Pad Length, Next Header가 암호화되며, 인증 데이터를 제외한 전체 ESP 패킷이 암호화된 후에 인증된다. ESP또한 AH와 동일하게 전송모드, 터널모드 2가지 모두에 동작된다. [그림 2]는 각 모드 상태에서의 IP 패킷의 변형을 보여준다[4].



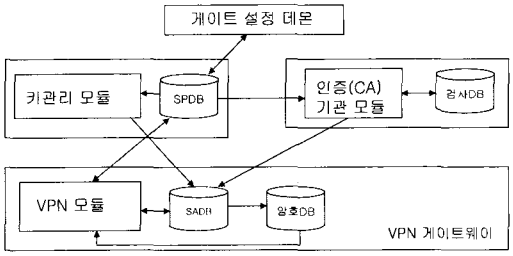
[그림 2] ESP 헤더 구조
[Fig 2] ESP header Architecture

3. 가상 사설망의 시스템

3.1 가상 사설망의 메카니즘 구조

VPN 인증기관 게이트웨이 설계모델의 [그림 3]은 게이트설정 데몬은 사용자 인터페이스와 드라이버의 동작 및 터널모드 회선에 관련된 내용 포함되어 있다. 키관리 모듈은 공개키를 기반으로 한 인증 시스템의 구현원리로서, 인증(CA) 기관에서 총괄적인 VPN의 관리를 수행하고, VPN 모듈 부분은 각각의 VPN은 하위 인증기관(Sub CA)과 등록기관(RA)을 통해서 VPN게이트웨이의 총괄적인 관리 감독 및 게이트웨이의 역할을 수행 할 수 있다. 각 VPN 게이트웨이의 등록정보는 VPN의 등록기관간의 교환과 마스터 인증기관의 데이터베이스에 저장되어 마스터 인증기관에서 총괄하게 된다.

인증기관으로부터 등록된 VPN 게이트웨이 정보를 총괄적으로 관리하며, 감사기록을 남김으로써 부인방지(Nono-Repudiation)역할을 함께 수행하게 된다. 인증기관에서는 등록기관의 등록정보를 VPN에 전달하고, 설정내용 및 사용자의 세션 키 관리와 터널링 프로토콜 등의 정보를 전달해준다.



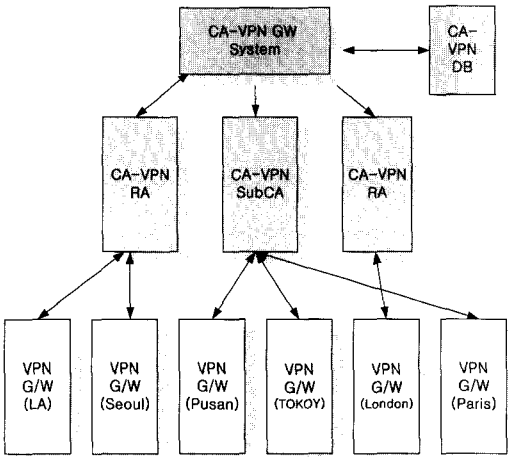
[그림3] 가상사설망의 메카니즘 모델
[Fig 3] mechanism model of VPN

또한 등록기관의 관리를 수행함으로써 마스터 인증기관의 부하를 감소시키는 역할을 수행한다. 등록기관은 VPN 게이트웨이의 등록을 대행하는 기능을 수행하고, 연결에 관련한 터널링 프로토콜, 암호화 알고리즘, 세션 키 등을 실제적인 상호 연결 관리를 하여, VPN 사용자에 대한 정보를 감사기록 한다.

3.2 CA-VPN에서 인증 시스템

PKI의 공개키 인증 시스템에서 VPN 게이트웨이의 기밀성과 인증에 의한 키 교환을 함으로서 사용자에 대한 신뢰가 확보되고, 시스템간의 키 교환 안정을 확보를 위해서 암호화하여 연결한다. [그림 4]는 CA-VPN의 인증 구조를 나타낸 것이다. 그리고 인증기관으로부터의 인증서 관리를 통해 특정 기간별, 사용자별 제한을 통해 공격자의 접속을 차단할 수 있다. CA-VPN에서 게이트웨이 운용관리시스템은 추적 및 관리와 방어를 함께 응용할 뿐만 아니라, 모든 VPN 사용자의 실시간 관리를 목적으로 하고 있다. VPN에서 게이트웨이의 기능으로는 VPN기능과 PKI기능들을 결합한 상호보완 된 보안기능들로 보다 안전한 패킷 데이터 송수신 및 관리를 할 수 있는 보안시스템을 구성한다[2]. 또한, CA-VPN에서 게이트웨이

의 제안은 앞으로의 VPN 사용자 급증과 오용 가능성을 고려한 것이다.



[그림 4] CA-VPN의 인증 구조
[Fig. 4] Certification Architecture of CA-VPN

기존의 키 교환방법이 아닌 인증기관을 통한 신뢰성 있는 사용자 인증과 세션을 성립에 따르는 정보 유출가능성을 배제하기 위해 공개 키 기반의 인증 시스템을 통한 응용에 대해 해결책이 필요하다. 이러한 키 관리의 취약성에 따른 보안과 사용자에 대한 인증을 위하여 PKI를 응용한 인증 키의 교환 및 인증서 발급을 통해 보안성 및 안전성을 향상시킬 수 있다.

(1) 인증기관의 운용관리

인증기관 및 등록기관 관리를 수행한다. 하위 인증기관과 등록기관들을 통합 운용관리 함으로써 인증서 및 인증서 폐지 목록 관리, 키 등의 인증에 사용하는 데이터를 일괄적으로 관리하고, 마스터 인증기관에 전송하여 DBMS에 저장 보관하도록 한다.

(2) 세션 키 관리 기능

접속자의 접속시간, 세션 키, 암호화 알고리즘, 터널링 프로토콜, 전송시간, 목적지와 출발지주소 등에 대한 정보를 등록기관 또는 하위 인증기관에 전송하고, 주기적으로 마스터 인증기관 데이터베이스에 보관한다. 차후 부인방지를 위한 감사기록 로그로써 활용할 수 있다.

〈표 3〉 DBMS의 구성 형태
〈Table 3〉 Organization Type of DBMS

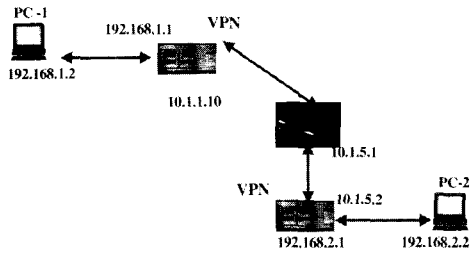
구 분	기 능
Certificate	CRL& Certificate Sub CA/RA information
Crypto Set	Cryto Algorithm AH Algorithm
Session Key	Key Manage Key Create/store Key log store
Log	Connection log Source/Destination IP & Port Keychange Algorithm
Tunneling Protocol	Tunneling Protocol Set Connection Port Set
Proxy Seting	Service Port Set Flag Set Realtime Status

- 키 관리 : VPN 통신을 하고자하는 사용자간의 세션 연결을 위한 세션 키의 사용자별, 네트워크 주소별 등의 정보를 포함하게 된다.
- 키 생성 및 저장 : 세션 연결에 필요한 세션 키의 생성을 인증서와 함께 사용자에게 분배한 시간과 유효성을 함께 포함하는 정보를 기록한다.
- 키 로그 저장 : 키에 관한 모든 접속 로그 및 사용자로그 기록을 총괄하여 저장한다.

4. 성능 평가 및 분석

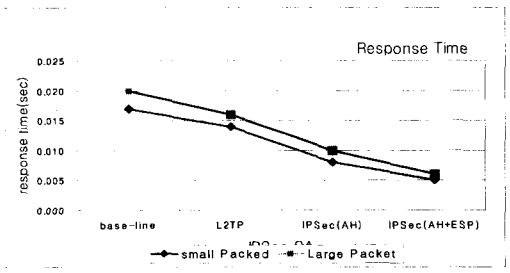
VPN 시스템의 하드웨어 구성 형태는 [그림 5]와 같다. 리눅스 서버를 통해서 VPN 게이트웨이를 구축하였고, 목적지 주소와 출발지 주소는 VPN 연결 사용을 원하는 사용자간의 설정된 주소로써, VPN 게이트웨이가 라우터 장비를 통해서 전달한다. 여기서는 계층2의 L2TP 프로토콜과

계층3의 IPSec 프로토콜에 의해서 터널링할 경우에 전달되는 정보의 성능을 파악하였다. 종단에 있는 VPN 게이트웨이로부터 전송되는 정보는 보안 알고리즘과 해당하는 계층의 프로토콜의 선택을 고려하여 데이터 캡슐화가 이루어진다.[11,12]



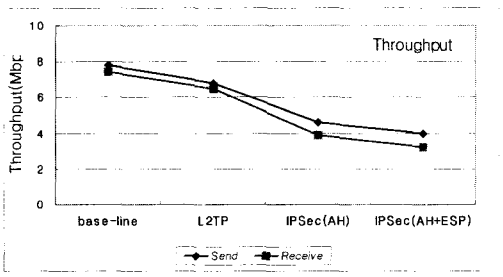
[그림 5] 하드웨어 구성도
[Table. 5] Hardware Organization

정보의 응답시간을 측정한 결과는 [그림 6]은 전송에 대하여 패킷의 크기(Packet Size)는 64byte과 128byte을 사용하여 15번 반복 테스트하여 평균으로 얻는 값을 표시한 것이다. 따라서 계층간 프로토콜의 터널링에 대한 반응시간이 base-line, L2TP, IPSec(AH), IPSec(AH+ESP)의 순으로 차이를 보여주고 있다. 이는 암호화와 캡슐화에 따른 시간의 차이를 볼 수 있고, 패킷의 크기가 적은 경우와 큰 경우와의 비율 차이를 보여주고 있다. base-line을 기준으로 패킷의 크기가 적을수록 응답시간이 빠르게 나타난다.



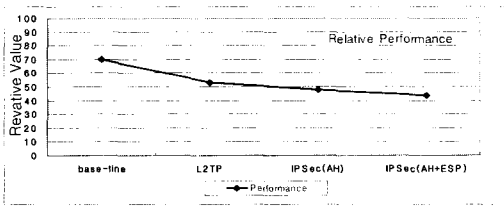
[그림 6] 응답시간
[Fig. 6] Response Time

정보의 처리량에 관한 결과는 [그림 7]에서 보는 것과 같다. 기본, L2TP, IPSec(AH), IPSec (AH+ESP)에 의해 패킷의 처리되는 량을 표시한 것이다. 암호화를 하지 않는 기본(base- line)이 속도가 빠르고, L2TP, IPsec(AH), IPSec (AH+ESP)에 의한 전송되는 순이다. 그러나 계층2와 계층3의 차이는 별차이를 보이지 않는다. 일반적으로 VPN구축은 L2TP 보다 IPsec 에 의한 네트워크 보안과 인증에 대한 표준화가 되어 있다. base-line을 기준으로 L2TP와 IPSec의 패킷 처리율의 차이는 10%의 범위 내에 있다. 즉, 송신보다 수신의 다소 빠른 것은 캡슐화된 과정이 역으로 이루어지기 때문이다.



[그림 7] 처리량
[Fig. 7] Throughput

정보의 상대적인 처리 성능은 [그림 8]과 같다. 암호화와 인증을 하지 않는 기본(base-line)을 기준으로 볼 때 계층2와 계층3 상대적으로 차이가 없다. 이는 컴퓨터의 CPU의 처리능력 향상으로 기인한다고 볼 수 있다. 네트워크에 구축된 장비와 발달된 컴퓨터기술의 접목으로 성능에 대한 차이는 무의미 한 것으로 생각된다.



[그림 8] 상대적 성능
[Fig. 8] Relative Performance

앞에서 살펴본 것과 같이 각각의 성능에 대한 평가를 종합해 보면 인터넷 네트워크 상에서 가상 사설망을 이용하면 정보를 안전하게 교환이 가능하다. 계층 2와 계층3간의 상대적인 성능에 대한 차이는 거의 없고, 응답시간과 처리량을 통해서 다소 차이는 있지만 보다 기밀성과 신뢰성이 필요한 네트워크 구축과 VPN의 활용할 경우는 암호화와 인증이 있어야 한다.

5. 결론

인터넷을 통한 정보 교환은 보안문제의 심각성이 대두되고 있으며, 보다 안전하고 신뢰성 있는 네트워크 구축에 대해한 신뢰성을 요구하고 있다. 인터넷 상에서 VPN구축은 계층간의 프로토콜 성능을 비교 분석한 결과는 계층 2인 L2TP은 계층 3 IPSec 보다 응답시간과 처리량이 다소 양호함으로 나타나고 있다. VPN 터널링 통해서 계층간의 프로토콜 적용은 사용자의 설정에 차이가 있으나 계층2가 계층 3보다 반드시 우수하다고는 볼 수 없다. 그러므로 계층간에 프로토콜에 관계없이 VPN을 구축함으로서 제 3자의 공격 가능성이 CA-VPN 게이트웨이에 의해서 접속이 차단할 수 있고, 해킹 및 접속시도에 따른 감사기록을 관리할 수 있어 침입경로 및 침입패턴으로 추적이 가능하다. 또 현재 사용중인 키 분배 메커니즘은 사용자 정보의 유출가능성으로부터 CA-VPN을 통해 스니핑 공격으로부터 보호될 수 있다. VPN의 구축은 암호화와 키 인증을 통하여 상호간 정보의 전송뿐만 아니라 상대측 이용자의 신원을 확인함으로써 VPN은 기밀성과 무결성을 기대할 수 있다.

※ 참고문헌

[1] W. Richard Stevens "Unix Networking Programming, 2nd Ed, Vol. 1, 1998.

[2] David McDysan , "VPN Applications Guide : Real Solutions for Enterprise Networks" Jonhn Wiley & Sons, Inc, 2000

[3] William Stallings, "Network Security Essentials : Applications and Standards " Prentice-Hall, Inc, May 1999

[4] S. Kent, R.Atkinson, "IP Encapsulating Security Payload(ESP)", 1998

[5] RFC 2408 Internet Security Association and Key Management Protocol(ISAKMP)

[6] AES Key Agility Issues in High-Speed IPSec Implementatins : Doug Whiting, Bruce Schneier, Steve Bellovin

[7] Modelling a Public-Key Infrastructure : Ueli Maurer

[8] IBM/Tivoli Technical Evangelist : Laura

[9] A Cyptographic Evalution of IPSec : Niels Ferguson, Bruce Schneier

[10] Performance Comparison of the AES Submissions : Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall

[11] IETP RFC 2661, Layer Tow Tunneling Procotocol "L2TP, 1999.

[12] IETF RFC 2401, Security Architecture for the Internet Protocol,1998

김 도 문

1984년 계명대학교 컴퓨터학과 졸업
1994년 숭실대학교 대학원 공학 석사
2000년 숭실대학교 대학원 컴퓨터학과 (박사과정 수료)
현재 : 동우대학 컴퓨터그래픽과 조교수
관심분야 : 네트워크보안, 암호학, 컴퓨터그래픽

전 문 석

1980년 숭실대학교 전자계산학과 졸업
1986년 University of Maryland, Computer Science(석사)
1989년 University of Maryland, ComputerScience (박사)
1989년 Morgan State Univ. 부설 Physical Science Lab. 책임 연구원
현재 : 숭실대학교 컴퓨터학부 정교수
관심분야 : 네트워크 보안, 암호학, 컴퓨터 알고리즘