情 報 保 護 學 會 誌
第 13 券 第 5 號, 2003. 10

IPSec VPNs vs. SSL VPNs

윤 재 호*, 권 태 경*, 천 동 현**, 임 선 간**

요 약

인터넷을 비롯한 대부분의 패킷스위칭 네트워크는 IP(Internet Protocol)을 기반으로 하고 있다. 그러나, IP는 기본적으로 보안에 취약하게 설계되어 보안이 필요한 통신에 사용하는데는 어려움이 있다. IPSec(IP Security)은 IP 트래픽에 대한 이러한 보안문제를 극복하기 위해 생겨났으며, 방화벽과 결합된 형태로 가장 널리 쓰이고 있는 VPN(Virtual Private Network) 제품의 하나이다. 그러나 IPSec의 문제점이 대두되고, Web-based Service가 영역을 넓혀가면서 기존의 웹보안프로토콜인 SSL이 VPN의 새로운 형식으로 나타나고 있다. 본 고에서는 IPSec VPN과 SSL VPN의 차이점의 분석하여 정리하고자 한다.

Ⅰ. 서 론

VPN(Virtual Private Network)은 공용네트워크환경에서 보안서비스 제공을 위해 가장 널리 쓰이는 제품으로 PPTP, L2TP, IPSec 등 다양한 프로토콜을 사용한다. 시장에 나와있는 VPN제품은 주로 기밀성 및 보안성, 그리고 터널링에 강점을 가진 IPSec 기반의 VPN이 주류를 이루고 있었는데, 호환성의 문제 및 DoS(Denial of Service) 공격, 접근제어(Access Control)의 상대적 취약성 등 IPSec의 문제점이 드러나면서 이를 위한 보완(IETF IPSec W/G)의 노력과 새로운 VPN 제품의 개발이 주된 연구대상이 되어왔다.

새로운 대안으로 제시되고 있는 SSL 기반의 VPN은 Web-base라는 강력한 장점 하에 이미 많은 브라우저 기반의 시스템이 지원하고 있어서 특별한 Client S/W의 다운로드 및 사용에 필요한 추가적인 지식이 불필요하기 때문에 IPSec 기반의 VPN이 가지고 있는 호환성의 문제를 쉽게 해결할 수 있으며 핸드쉐이크 프로토콜을 통한 강화된 접근제어 기능으로 보안성을 높였다. 특히 Web 기반(ex. Web Service)의 Business 영역이 확대되면서 기존의 Web Security를 대표해온 SSL VPN의 사용 전망이 밝을 것으로 예측되고 있다.

본고에서는 VPN의 기본적인 개념과 IPSec VPN, SSL VPN의 상호연동 및 모델구성, 확장성등의 측면에서 차이를 자세히 비교 분석한다. IPSec과 SSL의 기본적 설명은 생략한다.

Ⅱ. VPN(Virtual Private Network)

인터넷은 모든 사람이 공유하는 공용 네트워크이다. VPN은 이러한 인터넷을 사용자에게 사설망(Private Network)처럼 사용할 수 있도록 해주는 기술이다. 다음은 VPN정의의 한 예이다.

"A VPN(Virtual Private Network) is a private connection between two machines that sends private data traffic over a shared or public network, the Internet. This emerging technology lets organizations extend its network service over the Internet to branch offices and remote users creating a private WAN (Wide Area Network) via the Internet. The appeal of a VPN is the Internet and its global presence. Communication links can be done quickly, cheaply, and safely across the world."

출처 : http://archives.vpncon.com/whatarevpns.htm

* 세종대학교(jhyoon@kisa.or.kr, tkwon@sejong.ac.kr)
** 한국정보보호진흥원({dhchoen, seongan}@kisa.or.kr)

2.1 Private Network

VPN을 이해하려면 먼저 사설망(Private Network)에 대한 개념을 먼저 살펴볼 필요가 있다.

정보공유의 필요성 및 업무의 연속성 등 정보기반 구조를 위해 기업들은 인트라넷이라 불리운 내부망에 많은 투자를 해왔다. 하지만, 이런 내부망은 구축된 회사 내에서 만 효율적일 뿐, 원거리 접속에 대한 필요성은 충족시켜주지 못한다. 이를 해결하기 위한 방법으로 기업들은 독자적으로 PSTN(Public switched telephone network)을 이용한 Dial-up 접속 방식이나, 사설회선(Private Line) 방식등을 적용해 왔다. 이러한 방식을 Private Network이라 부르며[1] Private Network은 내부망에 있는 정보 및 자원을 내부에 있을 때와 동일하게 이용해야 하기 때문에 데이터 전송을 위한 안전하고 분리된 채널의 사용과 인증절차를 필수로 한다. 하지만 이러한 Private Network은 운영상의 고비용과 빠르게 변하는 기업의 요구사항(ex 회선증설 등)을 충족시키는데 문제가 있다. 이를 극복하기 위해 기존에 널리 연결된 공용 인터넷을 이용한 가상사설망(VPN)이 생겨난 것이다.

VPN은 일단 공용 인터넷망을 사용하기 때문에 운영경비가 저렴하며, 사설망이 안고 있던 이용 장소의 문제점도 탈피했다. 또한 암호적 기술을 이용한 데이터의 기밀성과 무결성을 제공하고, 인증과 접근제어를 통해 자원과 서비스의 사용을 제한한다. 기존의 사업영역이 공용 인터넷망으로 옮겨감에 따라 E-commerce에도 점차 적용영역이 확대 될 것이다.

VPN은 Private Network에서 강조된 보안을 위한 물리적 '분리'의 개념보다'안전한 터널의 형성'에 주안점을 두고 있다. 사설망의 경우 외부 접속이 필요한 곳마다 회선을 증설해야 하는 비효율적인 면이 있는데, VPN의 경우 기존에 연결되어 있는 공용망에서 터널링기법을 이용해 연결성과 동시에 보안서비스도 제공하여 준다.

2.2 Tunnel

일반적인 네트워크를 바라보는 관점은 topology와 architecture로 구별된다. topology는 게이트웨이나 루터라 불리는 컴퓨터간의 네트워크 연결 형태를 규정하는 것이고, architecture는 각 네트워크에서 데이터의 흐름을 규정하는 프로토콜들의 집합, 즉 프로토콜 Layer들에 대한 모델이다. Tunnel은 어떠한 가상 topology를 실제의 물리적 topology의 상위에 생성하기 위해 반복적으로 적용되는 하나 또는 여러 개의프로토콜 layer들로 architecture개념에서 정의된다. 터널링은 이러한 터널을 형성하는 것을 말하며, 모든 네트워크 Layer에서 가능하다. 하지만, 터널링은 Layer 2(link layer)와 Layer 3(network layer)에 가장 일반적으로 사용되며, 이로 인해 터널링을 사용하는 대부분의 VPN이 이 Layer에서 개발되어 왔다[1].

터널링은 다음과 같은 상황에서 유리하게 적용될 수 있다.

① 여러 개의 서비스가 하나 또는 이상의 traffic flow에 적용될 때, 터널은 서비스들이 적용되는 게이트웨이부터 원래의 traffic을 추출할 게이트웨이 사이에 형성된다. 암호화와 같은 보안서비스도 이 구간에 적용된다.

② 특정 도메인내의 주소들이 다른 곳에선 의미가 없을 때 적용된다. 예를 들어 인트라넷은 방화벽 안에서 종종 사설주소기법(private addressing)을 사용하는데 원거리에 존재하는 인트라넷간의 송수신되는 패킷들은 공용 인터넷망을 가로질러 전송될 수 있다. 이때 인터넷에서는 도메인 내부에서 사용된 사설주소(private address)는 전송(routing)과는 무관하다. 즉 터널은 인트라넷간의 사설주소를 숨기기 위해 형성된다.

③ 두 개의 도메인이 동일한 프로토콜을 사용하지만, 전송프로토콜은 다른 프로토콜을 사용할 경우 적용된다. 예를 들어 인트라넷간에 IPX(internet packet exchange)를 사용하는데 IP를 사용하는 공용 인터넷망을 통해 전송이 필요할 경우 터널링을 통해 IPX 패킷을 감쌀 수 있다(encapsulate).

Ⅲ. IPSec(Internet Protocol Security)기반 VPN

IPSec의 목표는 Host-to-host, subnet-to-subnet, host-to-subnet의 안전성을 보장하기 위한 것이다. IPsec은 모든 network traffic을 암호화 할 뿐만 아니라, 사용자가 마치 Internal Network에 있는 것처럼 LAN등의 resource를 이용할 수 있도록 해준다.

IPSec은 통신하는 서버에 맞는 특정 Client S/W을 인스톨해야 한다. 이것이 호환성에 걸림돌이 될 뿐만

아니라, Web에서 다운로드받는 이 S/W에 Trojan horse 라도 심어지면 문제가 심각해진다. 또한, 이 Client S/W는 인스톨된 특정 Laptop 혹은 Desktop에서만 서비스가 제공되기 때문에 이동성이 떨어진다.

대부분의 IPSeClient는 windows에서 구현되어 있고, 소수 몇몇의 client만이 Mac, Linux, Soralis 등을 지원한다.

Ⅳ. SSL(Secure Socket Layer)기반 VPN

4.1 IPSec과 SSL의 유사성

두 개의 암호프로토콜 모두 다양한 암호 알고리즘을 지원하며, 이 암호알고리즘은 데이터의 암호화는 물론 핸드쉐이크 방법을 통한 데이터 인증 알고리즘도 포함한다. IPSec과 SSL에서 지원되는 Cipher Suites는 모두 공개키 알고리즘을 기반으로 하고 있으며, 인증서를 이용한 PKI(Public-key Infrastructure)의 요소도 포함하고 있다.

4.2 Tunneling과 SSL VPN

터널링의 기본 개념은 network topology를 구성하는 것이기 때문에 Application Layer에서의 적용은 개념상 어려울 수도 있다. 왜냐하면, Application Layer는 컴퓨터간의 연결보다는 주로 자원의 관리에 중점을 두기 때문이다. 따라서 SSL VPN은 터널링이 제공해주는 2.1절의 세 가지 환경지원이 어렵다. 하지만, 필요한 자원에만 직접적으로 연결하여 핸드쉐이크에 의한 데이터의 기밀성 및 무결성, 그리고 접속 당사자의 인증 제공 기능은 터널링과 차별된 기능이라 하겠다.

4.2 SSL기반 VPN

SSL기반 VPN의 핵심은 Client application이 어느 누구의 컴퓨터에서도 가능하다는 점이다. 즉, web-browser를 사용하는 모든 프로그램에서 가능하다. 이는 IPSec VPN이 구현 서버에 따라 거기에 맞는 Client를 사용해야 한다는 점과 크게 대비된다. 또한, SSL은 두 application 간의 서로 통신하고 싶은 데이터의 traffic만을 암호화한다. 즉, 하나의 호스트에서 다른 호스트까지의 모든 트래픽을 암호화하는 것은 아니다.

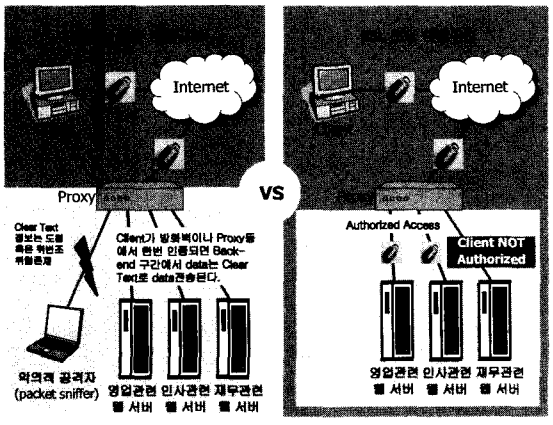
SSL VPN의 특징을 살펴보면 다음과 같다.

- No client-side software or hardware requirements
- Easy-to-use, easy-to-support Web interface
- End-to-End vs. End-to-Edge Security [그림 1] 참조

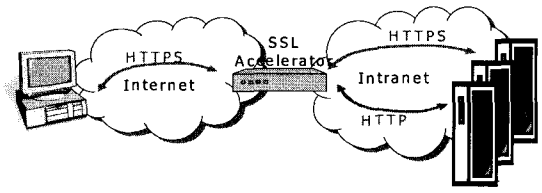
IPSec의 가장 큰 단점은 단지 client와 VPN 서버간에만 안전한 터널을 생성한다는 것이다. Client가 resource에 접근할 때 마치 같은 네트워크의 안에 존재하는 것처럼 취급된다. 이는 Client와 VPN 간의 안전한 connection은 단 하나 인데, 일단 IPSec VPN connection이 형성되면 internal network 상의 돌아다니는 모든 암호화되지 않은 data(ex.패스워드 등의 민감한 data)를 Entity가 획득할 수 있다. 즉, 진정한 end-to-end security는 제공하지 못한다. 하지만, SSL은 각각의 resource에 독립적으로 접근하여 보안채널을 맺음으로서 이러한 기능을 제공한다. 어떠한 internal network data도 clear하게 전해지지 않는다([그림 1] 참조).

상업적 측면에서 보면 현재 인터넷 네트워크 트래픽의 90%는 Web과 E-mail이므로 이동성과 안전성을 제공하는 SSL VPN이 IPSec VPN보다는 경쟁력을 가질 수 있다는 예측도 할 수 있다.

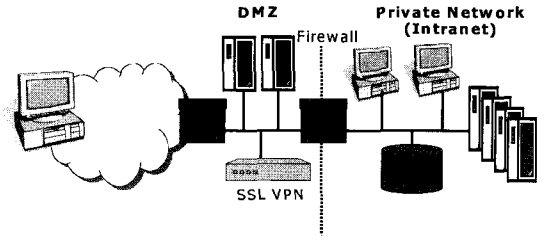
하지만 이러한 SSL도 심각한 문제를 가지고 있다. 가장 큰 문제는 성능의 문제이다. 예를들어 100명의 Client가 동시에 SSL VPN서버에 접속할 경우 Client는 1번의 공개키 연산(Key transport only-RSA, 인증서 검증 제외)만을 필요로 하지만, SSL VPN 서버는 동시에 100번의 공개키 연산을 해야한다. 이는 시스템 응답시간을 크게 저하시킬 수 있으며, 응답시



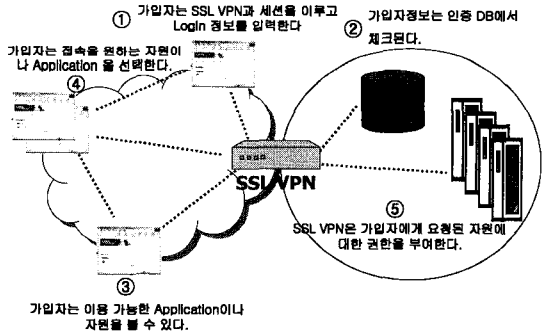
[그림 1] 보안연결구간 비교(SSL vs IPSec)



〔그림 2〕 SSL 가속기 구성위치



〔그림 3〕 SSL 가속기를 이용한 실질적인 구성예



〔그림 4〕 SSL 가속기를 이용한 Back-end Authentication

간이 상대적으로 빠른 IPSect VPN과 대비될 수 있는 약점이 된다. 이런 문제점 때문에 최근 대두되고 있는 것이 공개키 연산을 효율적으로 수행할 수 있는 SSL가속기의 개념이다(〔그림 2〕, 〔그림 3〕).

SSL가속기의 사용은 VPN 서버의 앞단에서 가장 시간이 많이 걸리는 공개키 연산의 효율적 수행과 back-end strong authentication을 지원하므로서 SSL VPN의 결점을 보완할 수 있다. 〔그림 4〕는 SSL 가속기를 사용한 back-end strong authentication을 제공하는 SSL기반 VPN 구성의 한 예이다.

V. IPSec기반 VPN vs. SSL기반 VPN

IPSec기반 VPN과 SSL기반 VPN을 비교하는데는 다음과 같은 4가지의 요소들을 고려해 볼 수 있다[4].

- Interoperability :
  · 지원되는 네트워크와 제품들의 상호연동 범위
- Layout and Security Features :
  · OSI model에서의 위치와 영향
- Scalability :
  · Capacity/load 가 성능에 미치는 영향
- The IPv6 Factor :
  · IPv6가 SSL와 IPSec에 미치는 영향

5.1 Interoperability

MS, netscape, apache등의 대형 Web-server 업체는 모두 SSL을 지원하고, Unix와도 쉽게 호환된다. 하지만, 다른 application에서 SSL을 사용하고 싶다면 SSL을 독자적으로 구현해야 한다. 이것은 SSL이 다른 application과 호환되지 않는다는 것을 의미한다.

현재 IPSec은 IPv6의 출현으로 IETF에서 네트워크 장비 및 PC의 다양한 벤더들이 지원하고 호환성을 가질 수 있도록 표준화 작업을 진행중이다. IPSec은 기존의 SSL이 가지고 있던 호환성 문제에서 자유로울 수 있는데 이유는, network layer에서 작동하기 때문에 개개의 application과는 독립적으로 작동하기 때문이다. 이론적으로는 이렇지만 현실에서 IPSec은 IETF 문서의 복잡성과 모호성으로 그다지 뛰어난 호환성을 제공해 주지는 않는다.

5.2 Layout and Security Features

두 개의 프로토콜 모두 암호에 독립적이다. 즉, Entity간의 협상에 의해 암호프로토콜을 정할 수 있으며(IPSec JFKr 제외), 세션이 언제라도 교환이 가능하다. 또한, 두 프로토콜의 가장 큰 차이점은 OSI layer에서 어디에 위치하느냐는 차이이다. 즉 SSL은 TCP위에 위치하기 때문에 패킷필터링과 다른 요소들(identity, application and/or service, authentication method, encryption 알고리즘, 날짜와 시간)에 의해 access를 제어할 수 있다. 이것으로 인해 IPSec보다는 보다 높은 Access control 기능을 제공한다. 하지만, 보다 높은 Layer에 위치한다는 의미는 더 많은 overhead 처리를 의미하기도 한다.

상대적으로 IPSec의 Access control은 단지 source address와 destination address, 그리고 port에 의해서만 제어된다. 이것은 핸드쉐이크 시간을 현격하

게 줄일 수 있다는 장점이 있지만, 특정 분야 즉, 높은 안전성의 access control을 요구하는 분야에서는 사용이 어려울 수 없다.

5.3 Scalability

SSL의 경우 확장이 용이한 편이지만, 전술한 바와 같이 remote end 가 늘어날수록 추가적인 처리능력이 요구되므로 응답이 느려질 수 있다. 이는 SSL 가속기 등의 Proxy connector의 효율적인 운영으로 보완이 가능하다.

IPSec의 경우 IP의 고갈로 인한 IP의 확장이 문제였으나, IPv6에서 해결될 것으로 보인다.

5.4 IPv6 Factor

IPsec의 완성은 IPv6의 사용으로 이룰 수 있을 것으로 보인다. 이는 IPv6의 보강된 보안기능으로 추가적인 파일의 다운로드 없이 보안 Protocol을 가입자가 사용할 수 있으며, IP의 고갈 문제도 해결될 것으로 보인다.

Ⅵ. 제품개발 동향

6.1 IPSec기반 VPN제품 현황

IPSec 기반의 VPN은 현재 가장 널리 쓰이고 있는 제품이다. 최근 들어 소프트웨어 중심의 제품들보다는 하드웨어 기반의 방화벽이나 게이트웨이 장비가 대두되고 있다. 이는 IPSec에서 필요로 하는 블록암호 알고리즘 및 해쉬알고리즘, 키 교환 알고리즘(IKE) 등이 빠른 처리를 요구하기 때문에 소프트웨어 구현만으로는 한계가 있기 때문이다. 적용방식을 보면 3Com이나 Cisco와 같은 네트워크 사업자에 의해 루터 기반의 VPN 장비나, 방화벽 업체에 의한 VPN 기능이 추가된 방화벽 제품, 또는 VPN 기능만을 제공하는 하드웨어 제품 등을 들 수 있다. 시장의 방향은 방화벽에 VPN 기능이 추가되고 게이트웨이와 루터의 기능이 추가된 일체형 제품들이 각광을 받고 있다.

6.2 SSL기반 VPN제품 현황

SSL 기반의 VPN 제품들은 대부분 기존의 SSL을 가속기와 함께 하드웨어 제품으로 구현하여 독립적으로 사용하거나, 방화벽과 함께 구성된 하드웨어 제품으로 구현하여 판매되고 있다. SSL은 기본적인 암호모듈이 무료로 공개되어 있어 누구나 이를 수정하여 사용할 수 있는 장점이 있다. 다음은 SSL VPN 제품을 판매하는 업체들이다.

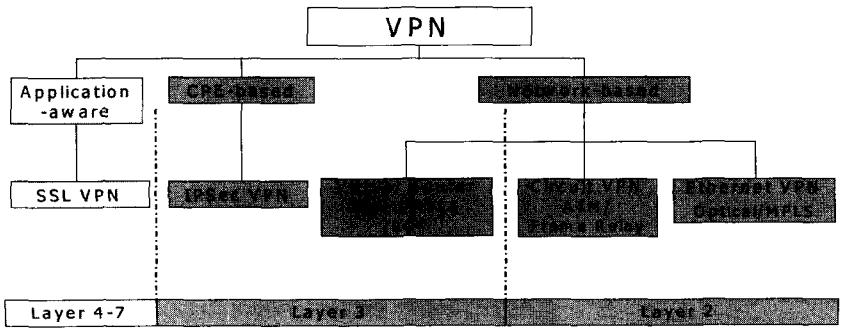
Aventail(www.aventail.com)
Neoteris Inc.(www.neoteris.com)
Netilla Networks Inc.(www.netilla.com)
NetSilica Inc.(www.netsilica.com)
Rainbow Technologies(www.rainbow.com)
Nortel Networks(www.nortel.com)-Alteon

Ⅶ. 결 론

암호화와 인증의 제공이라는 점에서 기존의 IPSec VPN과 대비되는 SSL VPN을 살펴보았다[비교표 참조].

다음의 그림은 Layer별 VPN 종류와 역할을 정리한 그림이다.

① Application-aware VPN : 외부 사업파트너의 extranet과 원거리 응용계층 접속(remote application access)에 적용될 수 있다.



〔비교표〕 - IPSec VPNs vs. SSL VPNs

항목	IPSec VPNs	SSL VPNs
Protection	IP 패킷	Application
Packet filtering	source/destination address, port	-
Performance	Faster/전체 connection에 하나의 handshake	각각의 Application connection에 handshake가 필요/more overhead
Platform	any system	client/server applications (espercially Web-based system)
Current Uses	현재 대부분의 VPN solution	Web-based Security
Scalability	Scalable on server-side, difficult to scale, clients connection 별 공개키 관리	Easy but, Session이 늘어갈수록 처리량이 늘어남
IPv6	Inclusion	-
Authentication	mutual/Digital certificate	mutual/Digital certificate
암호화	Strong Encryption/Depends on implementation	Strong Encryption/Browser based
Security	Edge to client/ Client-VPN gateway encrypted	End-to-end/ Client-resource encrypted
Cost	High/client S/W required	Low
Accessibility	Limited	Anywhere
Installation	Client-side S/W or hardware	Plug and play
UI	Training required (sometimes)	User friendly
Applications supported	All IP-based service	Web-enabled application, File sharing, E-mail
Users	Suited for internal company use	customers, partners employees, remote users, vendors

② CPE-based(Customer Premises Equipment) VPN : 각 인트라넷간의 연결 및 원거리 네트워크 계층 접속(remote network access)에 적용될 수 있다.

③ Network-based VPN : 보안업체들 보다는 주로 통신사업자(회선사업자)들에 의해 제공되는 서비스로 원거리 네트워크계층 접속(remote network access)에 적용될 수 있다.

위에서 보는 바와 같이 각 VPN은 고유한 특징을 지니고 있으며, 사용 목적도 분리되어 있다. 따라서 VPN의 적용은 필요한 요구조건에 맞게 구성되어야 하며, 적절한 VPN의 운영은 더 낳은 기업환경 정보기반구조(Information Infrastructure)를 조성할 수 있을 것이다.

향후 IPv6에 의한 IPSec의 VPN과 현재 사용의 편리성으로 인해 급부상하고 있는 SSL VPN의 시장 점유율 경쟁은 예측 불가능하며, 서로의 장단점으로 인해 4G에서의 All-IP(IPSec)와 Web-Service(SSL)처럼 끝까지 병존할 가능성도 보인다.

참 고 문 헌

〔1〕 Ruixi Yuan/W.Timothy Strayer, Virtual Private Networks, Addison-Wesley, 2001.

〔2〕 Manuel Gunter, Virtual Private Networks over the Internet, 1998 http://iamwww.unibe.ch/~mguenter/Reports/vpn.ps.gz http://citeseer.nj.nec.com/480338.html

〔3〕 SSL VPN vs. IPSec VPN White Paper, Array Networks, 2002 http://www.arraynetworks.net/

〔4〕 Christian Blaafjell et el., A Comparative Analysis of IPSec and SSL, http://citeseer.nj.nec.com/404774.html

〈著 者 紹 介〉

윤 재 호 (Jaeho Yoon)

1997년 2월 : 인하대학교 전자공학과 공학사
2000년 12월~현재 : 한국정보보호진흥원(KISA) 암호인증기술팀 연구원
2001년~현재 : 세종대학교 소프트웨어공학과 대학원
〈관심분야〉 PKI, 암호프로토콜

권 태 경 (Taekyoung Kwon)
종신회원

1992년 2월 : 연세대학교 컴퓨터과학과 졸업
1995년 2월 : 연세대학교 컴퓨터과학과 석사
1999년 2월 : 연세대학교 컴퓨터과학과 박사
1999년~2000년 : U.C. Berkeley Post-Doc
2001년~현재 : 세종대학교 컴퓨터공학부 소프트웨어공학과 조교수, 정보보호학회 편집위원, TTA 암호분과 특별위원
〈관심분야〉 정보보호, 암호프로토콜, 인증 및 키관리

천 동 현 (Donghyeon Cheon)
종신회원

1995년 2월 : 고려대학교 수학과 이학사
1997년 8월 : 고려대학교 대학원 수학과 이학석사
2001년 2월 : 고려대학교 대학원 수학과 이학박사
1999년 9월~2001년 8월 : 고려대학교 기초과학연구소 연구원
2001년 9월~현재 : 한국정보보호진흥원 암호인증기술팀 선임연구원
〈관심분야〉 암호학, 정보보호

임 선 간 (Seongan Lim)
종신회원

1985년 : 동국대학교 수학과 학사
1987년 : 서울대학교 수학과 석사
1995년 : Purdue 대학교 수학과 박사
1999년~2002 : 한국정보보호진흥원 선임연구원
2003년~현재 : 한국정보보호진흥원 암호인증기술팀장
〈관심분야〉 암호프로토콜, 정보보호 등