전송효율과 보안수준을 고려한 EDI 시스템과 VPN의 IPSec와 L2TP의 연동

최 병 훈† · 이 건 호††

요 약

인터넷을 통해 기업간 혹은 기업과 개인 간의 중요 업무에 관련된 정보의 교환이 점점 증가추세에 있다. 특히 ED의 발달로 인하여 기업의 업무처리의 시간단축과과 인건비 절감의 이점을 누릴 수 있으나 정보노출 및 보안사고가 발생되고 있다. 정보의 노출로 인하여 기업에는 막대한 손실 또는 생존위기에 이르게 하기도 한다. 흔히 IP의 부족현상과 정보의 암호화 및 인증화의 노출로 인하여 피해를 볼 수 있다. 따라서 본 연구에서는 전통적인 EDI방식과 VPN을 연동하고 정보의 중요도에 따라서 전송의 속도 및 보안의 강화를 구현한다. 이는 전통적인 EDI 방식과 VPN의 IPSec와 L2TP의 방식을 연동함으로써 사용자는 비용의 절감 및 정보의 보호 등의 이점을 얻을 수 있으며 기업 역시 비용절감과 암호화를 네트워크 계층에 따라 선택이 가능하도록 한다. 전송속도의 개선으로 인하여 기업과 사용자 모두 원활하고 안정적인 EDI 업무가 가능하다.

Interface of EDI System and VPN with IPSec and L2TP for Speed efficiency and Security Level

Byung-Hun Choi† · Gun-Ho Lee††

ABSTRACT

Electronic Data Interchange(EDI) between a number of companies goes on increasing on the internet. Although a conventional EDI system reduces business process efforts, time, resources, etc., important information is easily and frequently exposed by well trained hackers and crackers, which inflict a severe loss on the company and even put the company under a crisis. This study integrates the conventional EDI system and Virtual Private Net(VPN) to maximize an overall efficiency of speed and security in data transferring by the level of importance. The EDI system interfaced to IPSec and L2TP of VPN allows us to select two modes : the one focuses on a high speed with a low or a medium level security or the other does on a high level security with a low or a medium level speed. Both the company and the end users get a lot of tangible and intangible advantages by integrating the EDI system and VPN.

키워드 : EDI, VPN, 보안(security), IPSec, L2TP, ISAKMP, IKE

1. 서 론

네트워크를 이용한 기업간의 문서 및 정보 교환 으로 비용의 절감, 시간절약에 따른 내부 업무의 효율화 개선, 고객 서비스 향상, 거래당사자 간의 신뢰관계개선, 기업의 경쟁력의 강화 등의 효과와 이로 인한 매출액의 증가를 얻을 수 있다[1]. EDI시스템은 컴퓨터 통신망을 통하여 상거래 및 은행 업무에 관련된 전자문서를 교환하는 과정에서 중요한 정보가 노출될 위험이 있다.

정보의 보호 서비스에 대한 요구는 증가되고 있으나 모 기업과 지사와 연동성에 있어서 많은 비용의 부담과 보안의 취약성으로 인하여 그 발전의 한계에 도달하고 있다.

한국정보보호 진흥원의 정보보호관리 통제지침서중 문서의 중요성과 보안의 중요성, 금융 및 EC의 사기, 계약 분쟁, 정보의 노출 및 수정 등으로부터 보호하기 위해 신원확인, 무결성, 암호화, 부인방지 등의 대책을 수립하여 운영하도록 강조하였다[11]. 이에 따라 문서가 내포하고 있는 성격의 가중치로 하여금 문서관리를 효율적으로 보안하는 연구가 되고 있다[10].

VPN과 같은 정보보호제품 및 VPN 서비스를 제공하는 서비스는 기존 시스템이나 네트워크에 대한 외부로부터의 위험 침입을 차단시키는 기능이 수동적이다. 또한 방어적인 제품보다 시스템과 네트워크 자체의 안전성을 능동적으로 감지하는 기능을 가진 제품으로 변화하고 있다[2]. 특히 VPN의 기능은 정보보호 기술로 안전성이 매우 중요시되는

※ 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음
† 정 회 원 : 숭실대학교 산업기술정보대학원 산업정보시스템공학과
†† 종신회원 : 숭실대학교 산업 · 정보시스템공학과 부교수
논문접수 : 2004년 9월 3일, 심사완료 : 2004년 12월 28일

국방 분야의 C4I의 기술로도 사용하고 있다[3].

EDI를 사용하기 위한 전용선 망의 사용빈도수에 비해서 높은 가격과 전용선 IP의 포화상태 임에도 통신사용수는 증가추세에 있다.

이에 대안으로 VPN과 IPv6가 있으나 아직 IPv6에 관련하여 안정적인 장비 및 실제 상용화 되어 있지 않기 때문에 VPN이 대안으로 많은 관심의 대상이 되고 있다. IPv6가 상용화 되지 않은 상태이기 때문에 VPN의 상용화가 될 경우 모든 VPN의 장비를 모두 교체해야 하며 L2TP에 비해 IPSec 방식으로 만의 사용은 시간이 증가되는 단점을 가지고 있다[10].

인터넷 사용자중 VPN의 사용자는 날로 증가하고 있다. VPN은 공중망에서 전용선을 사용하는 것과 같은 효과를 나타내어 B2C, EC 등에서의 필수로 사용되고 있으며 홈 네트워크의 기술에서도 많은 연구가 되고 있다.

특히 유비쿼터스와 RFID등의 기술로 연계되어 각종 홈 네트워크 및 개인정보보호 분야에서도 연구 중이다[4].

EDI시스템의 적용에 대한 연구는 다양한 연구[5-8]가 있었으나 EDI 시스템과 VPN 연동에 대한 실용적인 연구는 이루어지지 않았다.

근래의 EDI 사용은 네트워크 통신망의 변화보다는 EDI 엔진 및 소프트웨어가 기존의 방식에서 xml을 이용한 xmlEDI의 방식을 사용하는 경우이다. 기존에 사용되고 있는 EDI의 방식보다는 안정성 및 보안성에는 보강되고 있으나 기존의 VAN을 이용한 EDI방식을 모두 VAN과 xml을 이용한 방식으로 바꿈으로서 소요되는 시간과 안정화 되는데 시간이 소요되며, 보안에 취약한 단점이 있다.

이는 EDI 시스템이 보다 편리하고 안정적으로 발전은 하여야 하나 비용과 기술에 취약한 중소기업의 입장에서 보안의 강화와 데이터 전송속도의 융통성의 결여로 도입에 어려움이 있다.

대표적인 EDI 시스템 서비스 제공 기업(www.samsung-networks.com)에서는 EDI 시스템을 web 또는 직접 시스템에 접속하여 사용하고 있다. 특히 무역의 Web xml EDI를 이용하는 것과 시스템끼리 접속하여 기업과 은행 간의 조회 및 이체 등의 업무를 시스템에 직접 접속하여 사용하고 있다[13].

현재 의료계 등에서 EDI 시스템을 도입. 계속 성장해 가고 있으며 연구가 되고 있다.

네트워크의 상태가 극히 불안하여 전송이 어려운 경우 시급히 전송해야 하거나 전송을 중간에 가로챌 가능성이 있는 경우 등 보안등급을 다르게 하여 데이터를 보내는 연구가 되고 있다[9].

IPSec 기반의 EDI 시스템의 사용현황 및 구축사례는 있으나 시스템 모델링에 관한 정보는 공개되지 않고 있다. 비즈메카(http://www..bizmeka.com) 등에서 의료비 청구를 위한 EDI 시스템을 VPN을 기반으로 사용하고 있으며 많은 기업들이 VPN방식으로의 서비스로 전환되고 있다. 미국의 경우도 기업간의 EDI 시스템을 VPN 환경으로 전환하고 있다[20].

Ford, GM, Krysler사로 구성되어 있는 ANX라는 세계 최대의 IPSec VAPN이 구축되어 있으며 900여 개의 부품 제조회사가 EDI를 사용하고 있다. 특히 IPSec을 이용한 EDI 시스템은 CPE VPN과 MPLS VPN의 두 결합되어 Single Vender에서 Multi Vender의 기업으로 구축될 전망이다[21].

EDI와 VPN의 IPSec와 L2TP의 연동에 관해서는 이용의 가능성 제시하고 있으나 이에 대한 연구결과가 발표 되거나 사용단계에 있지 않다. 따라서 본 연구에서는 기존의 IPV4에서 전용IP의 포화상태에 대한 하나의 해결책으로 보다 안정적이고 보안에 강력한 VPN과 EDI시스템의 연동 통하여 기존 방법들의 단점을 해소하고자 한다.

특히, EDI 문서를 전송함에 있어서 무조건적인 보안상태로 문서를 전송함으로 많은 시간을 낭비 하거나 혹은 시간적인 부분에 뛰어난 효과를 가지고 있으나 보안에 취약한 기존 시스템을 보완하여 다음과 같이 시스템 설계하였다.

첫째, 기존에 사용하던 EDI 시스템의 분석을 통하여서 문서의 중요도를 파악하고 분석하였다. 문서의 중요도를 파악하므로 기존에 문서전송을 하기 위한 소켓프로그램을 선택적으로 나눌 수 있는 방법을 제시하였다.

둘째, VPN장비의 IPSec와 L2TP를 이용하여 EDI 시스템에서 전송되고자 하는 문서의 중요도를 파악한 후 선택적 프로토콜의 구분사용으로 신속성 및 보안성을 보다 효율적으로 제고하고자 한다.

EDI VPN 시스템의 구축 시 EDI의 데이터 문서에 관하여서는 각 기업과 은행 간의 공통화 작업이 고려되어야 하며 또한 물류정보망의 구축 및 공유 혹은 물류정보의 공유, 물류표준화의 등이 선행되어야 한다[10].

2. VPN과 IPSec

VPN은 기업이나 개인이 인터넷을 경제적이고 안정적으로 통신망을 운영할 수 있도록 하는 솔루션이다. 인터넷기반 공중망을 마치 자신의 전용망처럼 사용하는 서비스로, 보편화된 인터넷이란 공중 네트워크에 가상적인 전용망을 꾸미는 것을 말한다. 즉, 인터넷과 같은 공용 인증망상에서 물리적인 네트워크의 구성과 무관하게 논리적으로 폐쇄된 사용자 그룹을 구성하여 다양한 기능의 서비스를 제공하는 네트워크의 한 형태이다.

본 연구에서는 전통적인 EDI 방식과 VPN의 IPSec와 L2TP의 방식을 연동함으로써 관리가 용이하여 관리비용을 절감하고 기존의 네트워크 확장의 어려움을 해소하며 저 비용으로 서비스를 제공하고 정보의 보호와 업무에 따른 전송속도의 융통성을 부여하고자 한다.

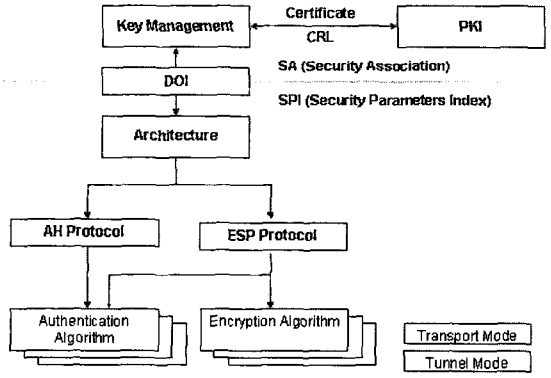
IPSec은 IP 계층에서 보안 서비스를 제공하기 위한 IP 계층 보안 프로토콜과 키관리 프로토콜로 구성된다. 이 두 프로토콜은 서로 독립적으로 설계되어 있으며 SA를 매개로 하여 연결된다.

IP 보안표준은 IP 패킷의 발신지를 인증하고 패킷 내용이 불법으로 변조되었는지 확인하는 무결성 서비스를 제공하는 인증보안메커니즘과 패킷의 데이터를 암호화함으로써 보안 서비스를 제공하는 암호화 보안 메커니즘으로 구성되어 있다[14].

요구되는 보안 기능에 따라 두 보안 메커니즘 중 필요한 것만 사용하거나, 동시에 사용될 수도 있다. 그리고 각 보안 메커니즘에서 필요한 보안 알고리즘과 기타 매개변수들은 별도로 보안모드에서 정의된다.

두 보안 메커니즘은 Transport 방식과 Tunnel 방식이라는 2개의 보안방식으로 각각 사용될 수 있다. Transport 방식은 통신하는 양, 호스트에 단말간 보안 기능을 제공하기 위한 것이고, Tunnel 방식은 양 호스트 사이에 위치한 보안 게이트웨이에서 보안 기능을 제공하여 안전한 가상사설망을 구성하기 위하여 사용된다.

한편 키관리 메커니즘은 통신하는 양 호스트가 사용할 보안 메커니즘, 키 값, 키 유효기간 등 보안 연결 설정을 위해 필요한 내용을 협상하고 필요한 경우에 보안 연결을 해제한다[14].



(그림 1) IPSec의 구조

3. 시스템 설계

본 연구의 하부 시스템은 사용자 인터페이스 부분과 입력된 자료를 처리하는 EDI 엔진부분, 그리고 처리된 EDI 데이터를 전송 하는 네트워크부분으로 구성되어 있다.

3.1 EDI 시스템 구성

EDI 시스템은 네트워크를 하여 EDI데이터를 전송할 수 있는 소켓부분과 VPN으로부터 받은 EDI데이터를 처리할 수 있는 엔진부분과 EDI문서가 각 디렉토리별로 쌓이거나 폐기 될 수 있는 부분이 있다.

EDI 시스템에서 나오기 전의 데이터베이스 문서는 중요도에 따라 1, 0의 값으로 나타낸다. TCP소켓 프로그램에서 세팅되어 EDI문서의 헤더부의 트랜잭션 ID의 값을 고유의 키 값으로 구분, 생성하여 EDI 시스템으로 전송된 후 VPN 장비로 보내게 된다.

데이터베이스에서 읽은 EDI문서의 중요도를 파악하는데 이때 반드시 송신측과 수신측의 IP Address를 알아 놓고 이 모든 송수신 측의 주소 또한 데이터베이스화 해놓아야만 생성된 소켓이 어느 IP address의 소켓을 생성할 것인가를 판단하여 보다 정확하고 데이터 손실률이 적은 회선에 시간적인 차이를 두고 보내줄 수 있게 된다.

3.2 VPN 망 시스템

3.2.1 L2TP구성

VPN장비로 전송되어진 EDI문서는 트랜잭션ID의 값이 0인지 1인지를 확인한 후 IPSec와 L2TP 전송방식을 택한 후 상대편의 VPN장비로 EDI문서를 전송하게 된다.

L2TP는 IP, SONET, ATM 등 여러 형태의 네트워크 상에서 PPP트래픽을 터널링 해 주는 프로토콜이다. L2TP는 PPP 패킷을 인캡슐하기 위한 PPP 인증, PPP 암호 제어 프로토콜 그리고 압축 제어 프로토콜 속성을 이어 받는다. L2TP는 또한 터널 끝점을 상호 인증하는 데 사용될 수 있는 터널인증 기능을 지원한다. 그러나 L2TP는 터널 자체의 보호 메커니즘을 정의하고 있지는 않다.

L2TP 보안 프로토콜은 키 관리 측면에서 확장 가능하여야 한다. L2TP 보안 프로토콜은 제어 패킷들에 대해 인증, 무결성, 그리고 재사용 방지 기능을 제공하며 제어 패킷을 보호할 수 있어야 한다.

데이터 패킷에 대해서는 무결성과 재사용 방지 기능이 제공되어야 하며 암호 기능도 제공할 수 있어야 한다. 또한 L2TP 보안 프로토콜은 키 관리 기능과 이의 확장성을 갖고 있어야 한다[15].

L2TP는 Microsoft사의 PPTP와 Cisco사의 L2F가 하나의 프로토콜로 함께 동작할 수 있도록 동의해서 표준화를 위해 IETF에 제시한 프로토콜이다.

L2F의 배경로는 layer2의 전송 패킷을 위한 암호화헤더를 정의하고, L2F 터널링은 IP에 속해있지 않고 다른 물리적 방식으로 동작 할 수 있게 한다.

Dialup 접속사용자들의 인증된 정보를 위해 PPP를 사용하고, 시작할 때 인증된 정보를 위해 TACACS+와 RADIUS를 지원한다. L2TP는 터널 내에서 연결을 정의하므로 PPTP와는 다르다. L2TP는 터널이 한개 이상의 연결을 지원하도록 한다. 사용자에 대한 인증된 정보는 첫 번째, 터널을 설치하기에 앞서 ISP에 대해 인증하고, 두 번째, 연결이 공통의 VPN장비에서 설치될 때 2 level이 있다.

PPTP처럼 인터넷을 통해 목적지에 tunnel 될 수 있는 Dialup 접속을 제공하기 위해 PPP의 기능을 이용한다[12].

L2TP는 L2F의 동작에 근거한 자체의 터널링 프로토콜

을 정의한다. L2TP는 PPTP처럼 PPP내 인증에 필요한 부분은(PAP, CHAP, RADIUS)을 포함한다. L2TP는 최종사용자와 L2TP간의 인증정보와 데이터의 무결성을 위해 PPP link상에서 IPSec 기반 인증정보를 적용하는 방법을 제안하였다.

3.2.2 IPSec 구성

IPSec방식을 사용하여 전송되는 EDI문서는 AH 또는 ESP를 요구하게 된다. AH 패킷과 ESP 패킷 처리순서는 다음과 같다.

-AH 패킷 처리순서

AH의 outbound 패킷 처리의 순서는 SA 검색을 한다.

(가) AH를 처리하기 위한 SA를 찾는다. SA에는 AH에서 사용하는 인증 알고리즘과 키, ICV의 길이, ICV를 계산할 때 고유번호를 포함시켜 Anti-Replay Service를 제공할 것인지의 정보가 정의된다.

그 다음 고유번호가 생성하게 되는데 해당되는 SA의 고유번호를 하나 증가시키고 반복되지 않는지 확인한다.

(나) ICV 계산을 한다.

AH의 ICV는 IP 헤더에서 변경할 수 없는 필드와 변하기 쉬운 필드가 있지만 상대 호스트에서 그 값이 예측 가능한 필드, 상위계층 프로토콜 자료에 대해서 계산되며 IP 헤더에서 변하기 쉬운(mutable) 필드와 AH의 인증정보 데이터 필드는 0값으로 지정된 후에 ICV를 계산한다.

(다) Inbound 패킷 처리의 순서는 먼저 재조립되는 부분(Reassembly)으로 AH를 처리하기 전에 IP 절단 및 분열된 패킷인 경우에 패킷을 재조립한다.

SA 검색은 수신 IP 패킷의 목적지 IP 주소와 SPI값을 이용하여 사용할 SA를 결정한다. 만약 사용할 SA가 없는 경우에는 IP 패킷을 버리게 된다.

고유번호 검사는 해당되는 SA가 Anti-Replay Service하는 경우에는 수신된 AH의 고유번호가 중복된 것이 아닌가 확인한다. 확인을 위한 윈도우가 SA내에 유지되며 윈도우의 크기는 64이다. 수신된 고유번호가 윈도우에서 유지하는 최소값보다 작거나 이미 수신된 고유번호인 경우에는 해당되는 IP 패킷을 버리게 된다. 수신된 고유번호가 윈도우에서 유지하는 최대값보다 큰 경우에는 ICV확인을 한 후에 윈도우를 변경한다.

ICV 계산은 수신된 IP 패킷에 대해 ICV를 계산하여 이를 수신된 ICV값과 비교한다. 두 값이 동일한 경우에 IP 패킷을 정당한 것으로 받아들이고, 반대로 두 값이 서로 다른 경우에는 해당되는 IP 패킷을 버리게 된다.

-ESP 패킷 처리순서

ESP의 Outbound 패킷 처리의 순서는 SA 검색이 있다.

(가) ESP를 처리하기 위한 SA를 찾는다. SA에 ESP에서 사용하는 암호 알고리즘과 키, IV의 사용 여부, ICV의 사용여부와 사용할 때의 ICV의 길이, ICV를 계산할 때 고유번호를 포함시켜 Anti-Replay Service를 제공할 것인지의 정보가 정의된다.

고유번호생성은 현재 사용하는 ESP가 인증기능을 제공하고 있고 Anti-Replay Service를 제공하는 경우에 해당되는 SA의 고유번호를 하나 증가시키고 고유번호가 반복되지 않는지 확인한다.

(나) 패킷의 암호화부분이 있는데 Transport Mode인 경우에 원래의 upper layer protocol 정보를 ESP Payload 내에 암호화(encapsulate)하고 필요한 자료의 채움과 ESP Trailer를 추가한 후 그 결과를 암호화한다. Tunnel Mode인 경우에는 원래의 IP 패킷 전체를 암호화한다.

(다) ICV 계산은 ESP가 인증기능까지 제공하는 경우에는 인증화 데이터(Authetication Data)를 제외한 부분을 먼저 암호화한 후에 ESP Header와 ESP Payload에 대한 ICV를 계산한다. 이 때 인증화 데이터는 암화화 하지 않으므로 MAC함수가 사용된다.

분열된 상태(Fragmentation)는 ESP를 생성한 후에 필요하면 IP 분열상태로 한다. Inbound 패킷처리는 재결합(Reassembly)상태가 있는데 ESP를 처리하기 전에 IP 분열상태로 된 패킷인 경우에 패킷을 재결합한다.

SA 검색은 수신된 IP 패킷의 목적지 IP 주소와 SPI값을 이용하여 사용할 SA를 결정한다. 만약 사용할 SA가 없는 경우에는 IP 패킷을 버리게 된다.

고유번호 검사는 현재 사용하는 ESP가 인증기능을 제공하고 있고 Anti-Replay Service를 제공하는 경우에 수신된 고유번호가 중복된 것인지 확인한다. 이 때 사용하는 윈도우의 크기는 64이다.

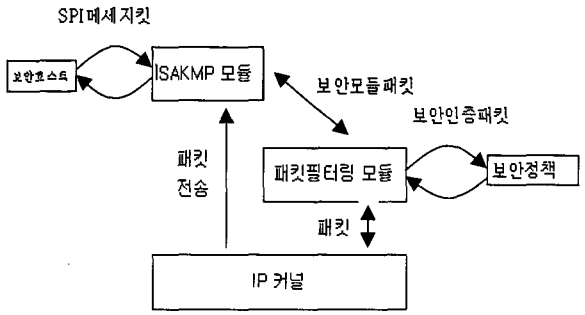
다음은 ICV 검증이다. 현재 사용하는 ESP가 인증기능을 제공하는 경우에 수신된 ESP 패킷에 대해 ICV를 계산하여 이를 수신된 ICV값과 비교한다. 두 값이 동일한 경우에 IP 패킷을 정당한 것으로 받아들이고, 반대로 두 값이 서로 다른 경우에는 해당되는 IP 패킷을 버리게 된다.

패킷 복호화는 SA에서 정의된 키로 ESP Payload를 복호화 한다.

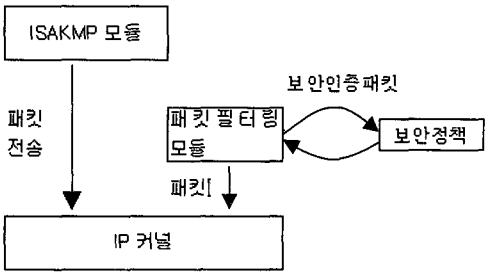
Inbound 패킷 처리는 (그림 2)와 같이 수신된 ISAKMP 패킷은 필터링 모듈에 의해 바로 IP 커널에 전달된다. 단, 보안정책의 제어 없이 보안호스트 체크(isakmp_filter)만으로 ISAKMP 모듈에서 처리할 패킷과 바이패스해야 할 패킷이 결정된다. 단, Center NAT 기능이 작동된 경우는 바로 바이패스하지 않고 보안정책에 따라 처리한다.

ISAKMP 메시지 전송 시 인증 상대에 대한 정보가 없는 상태에서는 인증을 유발한 응용 세션의 목적지로 패킷을 전송하게 되는데, 이러한 메시지로는 인증 시작시의 ID 요청 메시지와 수신 AH, ESP 패킷에 대한 가치가 없는 SPI

(Invalid SPI) 메시지가 해당된다. 따라서 수신 ISAKMP 패킷 중 보안호스트로 오는 패킷은 VPN보안장비가 직접 처리해야 하므로, Inbound ISAKMP 패킷에 대한 보안호스트 체크가 필요하다.



(그림 2) Inbound 패킷 처리과정



(그림 3) Outbound 패킷 처리과정

L2TP와 IPSec의 장단점은 다음과 같다.

〈표 1〉 L2TP와 IPSec의 장단점

구 분	L2TP	IPSec
장 점	- 단순함(Simplicity) - End-To-End 압축 및 암호화 - 시간적 절약	- 확장성 우수 - 보안성 우수 - 신뢰성 우수
단 점	- 확장성, 보안성, 신뢰성 미비 - PPP Payload 형식만 지원	- 보안화 암호화에 따른 시간소요

3.2.3 IPSec에서 IKE(Internet Key Exchange) 절차

IKE는 키교환, 보안서비스 협상 등을 ISAKMP를 사용한다.

IKE교환의 결과인증키와 협상된 보안서비스 (SA)가 생성된다. IKE는 ISAKMP의 Phase1, 2를 사용한다. Phase1은 IKE SA를 Phase2는 IKE SA를 이용하여 IPSec SA를 생성한다.

IKE는 IKE SA에 대한 속성을 정의하며 IPSec SA에 대한 속성은 DOI에서 정의하고 있다. DOI에서는 IKE가 Phase2 단계에서 협상할 Potional, Required 속성을 정의한다. IKE는 두개의 Phase1 교환과 한번의 Phase2 교환, 두 번의 내부교환을 정의한다. Phase1 교환에서는 ISAKMP의 정책보호 교환(Main Mode) 접근교환(Aggressive Mode)를 이용한다[18].

Phase 1의 정책보호 교환, 접근교환 모드는 두 Peer 사이에 메시지 소스인증, 메시지의 무결성과 환경을 제공하기 위해 사용하는 인증키들과 IKE SA의 설정과 같은 동일한 결과를 수행하며 다른 교환 전에 선행되어야 한다. Phase2 교환에서는 빠른 모드 교환을 정의하고 있으며 IPSec에 대한 보안서비스를 협상한다. 나머지 두 개의 교환은 IKE Peer가 통신 시 발생한 오류, 상태정보, 새로운 그룹교환 등 정보를 교환하는데 사용한다. IKE SA는 IKE SA와 인증키를 생성하기 위해 다양한 매개변수의 키를 갖고 있으며 각 매개변수에 대한 속성과 값을 정의하고 있다.

각 Peer는 암호화 인증을 위해 서로 속성과 값을 협상해야 한다.

매개변수의 값은 보호에 뒤따른 값이라 하며 ISAKMP SA Payload에 포함되어진다. 또한 각자의 속성들은 교환 Payload에 포함되어 진다[18].

4. 기능설계 및 분석

4.1 기능설계

대부분의 EDI업무는 전문과 같이 중요도가 높은 것과 통보 및 조회 등의 중요도가 낮은 업무가 있다. 업무의 중요도 보다 조회 등 빠른 시간적인 작업을 요구할 경우에 암호화, 인증화의 과정을 거쳐는 시간의 지체보다는 빠른 대응이 업무의 효율성을 높일 수 있다.

이때 중요도가 높고 낮음을 판단할 때는 양사간의 전문 포멧을 추가 또는 수정 시에 내용 등의 동의를 얻어서 나누어 중요도에 따라서 전문의 공통부 부분을 데이터베이스화 한다.

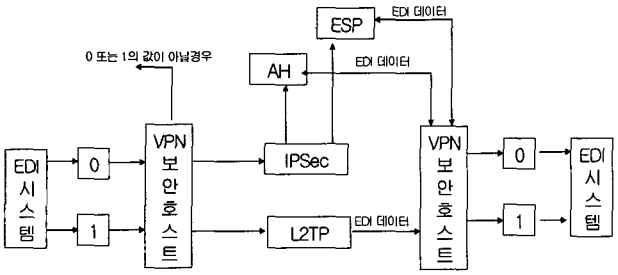
전문의 발송 시 전문의 헤더부에 따라서 IPSec 전송방식으로 보낼 것인지 L2TP방식으로 전송할 것인지를 판단, 시간과 보안적인 측면 두 가지로 구분한다.

EDI전문발송 시스템에서 어떤 내용의 전문을 파악한다. 업무의 중요도에 따라서 EDI전문의 해더부 즉, 공통부에 포함해야할 고유의 ID값을 데이터베이스에서 제공해 준다. 이 고유의 트랜잭션ID값은 EDI문서의 해더부 부분에서 트랜잭션ID값으로 구분되어서 전문이 발송실에 송신측과 수신측의 환경에 서로 맞추어져야만 된다. 이때 트랜잭션ID의 값에 0의 값이 추가가 되면 중요도가 높은 전문으로 인식하여 VPN장비에서는 IPSec 기반의 터널로 전송이 된다.

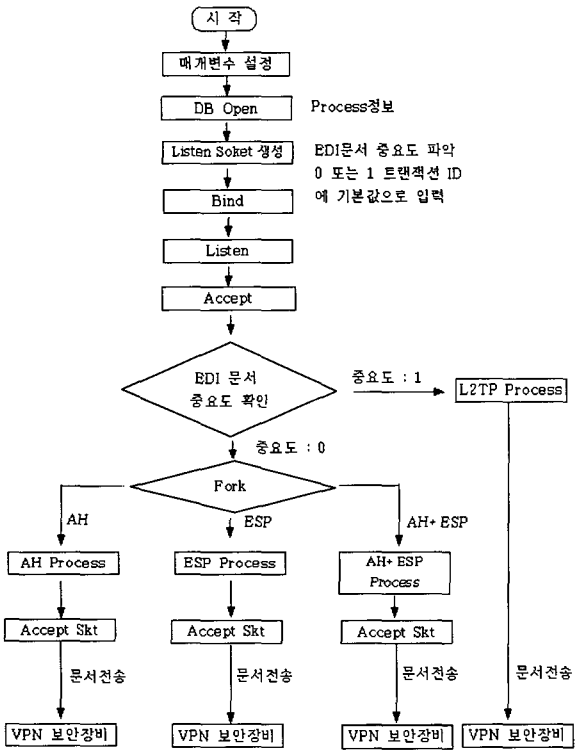
이때 IPSec기반의 터널구성이 이루어진 후 EDI문서에 AH+ESP해더로 인하여 암호화와 인증화 과정을 거치게 된다.

또한 EDI문서의 트랜잭션ID의 값이 1이면 조회 등 중요도가 낮은 문서로 인식하여 L2TP기반의 구성된 터널로 인하여 수신측의 VPN장비로 데이터를 전송하게 된다. 이때

트랜잭션ID의 값에 0 또는 1의 값이 함께 전송되어 지는데 TCP/IP기반의 소켓 프로그램에서 부과가 된다. (그림 4)는 전체적인 구성도를 나타내고 있다.



(그림 4) EDI와 VPN보안호스트간의 전체구성도



(그림 5) 시스템처리 순서도

기능설계는 다음과 같다

(가) 소켓 알고리즘

```
IF(트랜잭션 ID = 0){
   Client, Center 간 Tunnel 맺는다.
   EDI 전문에 IPSec AH + ESP 헤더 공간 확
   보 및 헤더복사
  IF(TCP/IP 연결이 되지 않은 상태)
     IP와 PortNO를 이용 해당사용자와 연결.
  IF(사용자 Code Type ='E'(EBCDIC코드)){
  ASCII를 EBCDIC코드로 변환하고 전문을
  해당사용자에게 송신.
IF(송신오류 발생) 전문을 폐기하거나 반송처리.
  }
ELSE IF(트랜잭션 ID = 1){
   EDI 전문에 L2TP 헤더 공간 확보/헤더복사
   IF(TCP/IP 연결이 되지 않은 상태)
      IP와 PortNO를 이용 해당사용자와 연결.
   ELSE Tunnel 구성 비보안 호스트로 인식
   세션 연결 안됨
}
```

(나) EDI처리 알고리즘

```
IF(요구전문과 같지 않으면 보관전문){
  해당 메세지를 특정 디렉토리(사용자별)에 저장
  한다.
  요구전문을 응답전문으로 바꾼 후 요구전문 송
  신자의 메세지 큐에 등록한다.
  }
ELSE{
  IF(요구전문 && (보관전문 or 응답전문)){
    IF(해당 사용자와 연결이 되어 있지 않음)
      해당 소켓프로세스 정보를 참조하여 연결.
    IF(사용자의 Code Type이 'E'(EBCDIC)
      ASCII를 EBCDIC로 변환하고 전문을 해당
      사용자에게 송신.
  }
} // End of IF
IF(보관전문){
  송신을 실패하면 보관횟수 1추가 하고 메세지
  특정 디렉토리(사용자별관리) 에 다시 저장.
  IF(횟수 > 3(P04)) 전문을 해당 디렉토리에
  보관횟수를 'P01'로 하여 저장.
ELSE IF(응답전문)  전문을 폐기.
} // End of IF
```

4.2 구현환경

EDI 데이터 전송 PC 2대를 사용하였으며, OS는 2000, 데이터베이스는 MS-SQL2000, CPU는 인텔 펜티엄4 2.66GHz, CACHE는 512KB, HardDisk/RAM은 80GB/256을 각각 사용하였다. 또한 EDI 처리엔진을 위해 OS는 UNIX, 데이터 베이스 Oracle, CPU는 750 MHz 2 CPU, CACHE는 1024 GB 그리고 HardDisk/RAM은 2*36 GB/4 GB을 각각 사용하였다.

VPN 보안장비(128MB)는 50,000 세션/4,000유저, VPN장비-to-VPN장비는 등록 확인된(L2TP) 128대, 보안정책으로는 SPD=1000개, NAT=500개, TC=100개, 호스트는 호스트 SPD=200개, SAR=20개를 각각 사용하였다. 네트워크는 KT ADSL 통신회선 사용하였다.

EDI 시스템 구축을 위해 X400과 연동할 수 있는 UNIX용 UA를 구현한다. HP, RS6000, SUN 등의 여러 UNIX System에서 사용이 가능하며, 통신프로토콜은 TCP/IP를 중점적으로 이용하였다.

TCP/IP로 통신환경을 설정한 후 사용자와 서버간의 연결은 VPN을 이용하며 VPN대 VPN의 부분은 IPSec, L2TP를 이용하여 보안 및 데이터 손실률, EDI전문의 이동시간을 기준으로 측정하였다. Unix사용자 환경에서 수행에서 하였다.

```
[2004/10/20 15:11:17] [INF] 전문 Recedive!(길이=311)[TRF 10000
    STTRF10000 00020024 204100100100011120041120151123000O]
[2004/10/20 15:11:17] [INF] Send A차![0]
[2004/10/20 15:11:17] [INF] [13980049] [SHBAFB01 → ServerTCP]
    TCP 응답전문 수신 성공!(길이=311/전문=TRF10000 STTRF10)
[2004/10/20 15:11:17] [INF] [13980049] [ServerTCP → Q_HVBBFB01]
                                메시지큐 Write 성공!(길이=341)
[2004/10/20 15:11:17] [INF] [13980049] DB
                                메시지큐 Write 성공!(길이341)
```

(그림 6) 기업과 은행간의 EDI데이터

(그림 6)은 은행과 기업간의 EDI문서이다. 원장변경사항에 응답전문으로 거래계좌번호, 거래점 GIRO코드, 거래금액, 입/출금자 성명, 어수번호 등이 기재되어 있다.

4.2 시스템 분석

100개의 EDI 데이터를 전송, 데이터베이스에서 EDI시스템으로의 TCP소켓 접속가능 여부와 전송되어진 EDI데이터의 전송시간, 실패확률, 패킷 등을 분석하였다.

EDI데이터의 중요도를 데이터베이스화하여 각 EDI전송 PC에서 VPN보안장비로의 접속여부를 확인, 이에 L2TP를 이용한 방식과 IPSec의 전송방식중 시간과 보안의 중요도를 파악한다. 이때 전송이 실패된 EDI데이터의 패킷을 캡쳐하여 분석한 후 패킷의 차이점을 비교하였다.

4.3 소켓접속 결과

EDI전송 PC에서 VPN보안장비로의 접속여부는 데이터를 전송하기 전 접속이 한번 이루어진 상태에서 EDI데이터를 전송하므로 무리 없이 접속되었다.

기존의 전용선 사용비용을 절감하여 EDI데이터의 처리시간의 이점을 얻을 수 있다.

전용선에 비해 상대적으로 저렴한 사용료임에도 회선의 품질 및 안정성에 대해서는 기업전용선에 전혀 뒤떨어지지 않기 때문에 VPN 전용선 사용은 증가추세에 있다. 특히 한국의 경우 2003년 중반 이후에 400개 중소, 벤처기업의 패턴을 분석해 보면 200여 회사가 기존의 전용선 방식에서 VPN 전용선으로 전환하여 사용하고 있다.

하지만 자료나 문서가 EDI 시스템을 벗어나 네트워크 통신망을 통과하는 과정에서는 보안의 많은 문제점이 있다.

따라서 본 연구는 단순 연결방식인 기존 EDI방식과 xml로 구성된 EDI의 방식과는 확실한 차이점이 나타나 있다.

문서의 중요도 및 속도적인 부분에서 차별화를 두어서 안정성 및 보안성을 강조하였다.

4.4 기존의 시스템과의 비교평가

<표 2>에서 S사에 등에서 사용 중인 기존방식[9, 18]과 본 연구의 사용 환경을 비교하였다. 기존의 EDI 전송방식에 비해 상대적 장점은 무엇보다도 비용을 현저히 절감 할 수 있다는 것이다. 또한 전송오류가 발생할 시에는 기존의 방식으로는 X.25회선에서만 패킷을 볼 수 있었으나 별도의 분석 장비를 가지고 확인해야 하므로 비효율적이며 비용이 추가로 소요되어야 한다. 이에 VPN 보안호스트를 사용하므로 자체적으로 분석과 원인을 할 수 있으므로 보다 빠르고 안정적인 대책을 세울 수 있다.

〈표 2〉 기존의 시스템과 본 연구의 비교

구 분	기 존 방 식		본 연구
	VAN EDI방식[9]	기존 VPN EDI[18]	
네트워크망	TPC/IP, X25, SNA, VAN업체회선 사용료	TCP/IP	TCP/IP (ADSL사용가능)
프로토콜	X.25, VAN	IPSec	보안등급에 따른 IPSec, L2TP 선택적 프로토콜
보안성	네트워크상에서의 보안의 취약함	AH, ESP에 따른 보안성 강화	AH, ESP에 따른 보안성 강화
장애에 따른 분석	VAN 사를 통한 내용분석(자체 패킷상으로는 분석 불가)	VPN 보안호스트로 패킷 자체분석	VPN 보안호스트로 패킷 자체분석
패킷분석	자체분석 불가	VPN보안호스트 자체 판독 가능	VPN보안호스트 자체 판독 가능
호완성	양쪽사용자의 패킷설정으로 보완성에 약하다	단순회선으로 사용하므로 호완성에 강하다	선택적 모듈화로 인하여 이식성가 호완성이 강하다
비 용	전송된 데이터에 따른 비용지불	VPN전용회선 약45,000원	ADSL 약 20,000원
장 점	- 추가 개발비용이 들지 않는다 - VAN업체를 통하므로 장애의 추적이 가능하다	- VPN장비로 인한 ADSL 사용료에 따른 비용절감 - 보안등급이 높다 - 데이터베이스가 단순하다.	- 보안등급에 따라 전송으로 보안 등급이 강화된다. - 보안등급이 낮은 경우 불필요한 시간을 해소 할 수 있다. - 모듈화로 인하여 보안의 등급을 세분화 할 수 있다
단 점	- VAN사용 및 장비비용이 비싸다. - VAN업체의 의존성이 높다.	- L2TP 또는 IPSec 중 한 가지 전송방식만 가능하다.	- 서비스 포트의 중복이 일어날 수 있다.

네트워크 상황에서 기존방식으로는 TCP/IP 및 X.25, SNA방식을 함께 사용하고 있으며 VAN업체를 통하여 전송되어지므로 이에 따른 비용 또한 적지 않게 들어가고 있다.

이에 VPN호스트를 사용하므로 TCP/IP방식의 ADSL 회선을 사용가능하므로 X.25, SNA, VAN업체 수수료 및 사용료 등을 지불해야 하지만 본 연구에서는 ADSL 비용만 지불하면 되므로 차액만큼의 비용절감 효과를 갖는다.

본 연구의 L2TP를 이용하여 데이터를 전송 시에는 전송시간을 단축 할 수 있다. 즉, 단순 계좌조회 및 데이터의 처리결과 조회 등은 EDI문서의 중요도가 낮으므로 L2TP통신방법을 이용하여 보냄으로 수신측에서 보다 신속한 결과를 받는 것이 효율적일 것이다.

IPSec를 이용한 EDI데이터 전송방식은 신속함 보다는 안전한 방식으로 암호화와 인증화의 과정을 거치도록 한다.

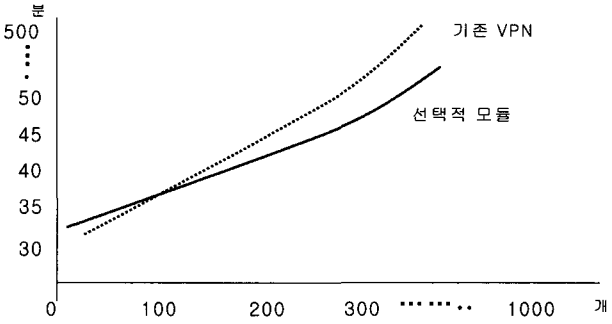
〈표 3〉 데이터 전송시간 비교

단위 : 분

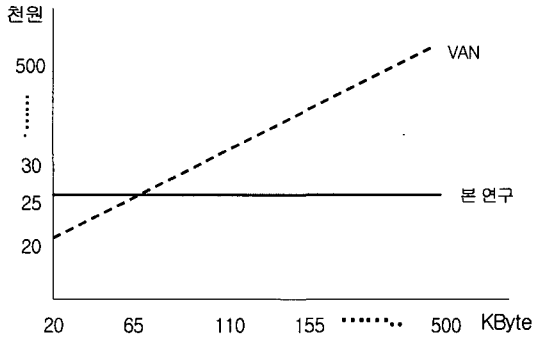
구 분		기 존 방 식		본 연구
		VAN EDI방식	기존 VPN EDI	
데이터 전송	1	37	38	37
	2	37	39	38
	3	36	38	36
	4	37	37	36
	5	37	38	36
	6	38	38	36
	7	36	38	35

<표 3>에서 데이터 전송시간 비교하였다. 기존에 VAN을 사용하여 데이터를 전송하는 경우 데이터의 암호화를 하지 않으므로 기존의 VPN을 사용하여 전송하는 EDI 시스템에 비해 보안에 취약하다. 또한 VAN을 사용하여 데이터를 전송하는 경우 데이터 전송량에 따라 비용이 소요되며 TCP/IP 전용선을 사용하는 경우에 비해 많은 비용이 소요 된다. 기존 VPN EDI를 사용한 경우 IPSec기반의 전송방식을 사용하며 IPSec과 L2TP의 선택적 방식을 사용하는 것보다 많은 시간이 소요된다. 이는 IPSec 기반이므로 암호화와 인증, 복호화를 시키는데 발생되는 시간이 소요되어 보안의 중요성이 다소 낮은 데이터 일지라도 많은 전송시간이 소요되기 때문이다.

(그림 7)은 EDI 데이터 전송량과 시간과의 관계 나타내고 있다. VAN을 사용한 EDI 데이터 전송 시 전송양이 적은 경우 선택적 모듈을 사용하는 경우보다 다소 빠른 처리가 되고 있다. 그러나 EDI 데이터의 전송량이 증가됨에 따라 VAN을 이용한 전송시간에 비해 VPN을 이용한 EDI 데이터 전송방식의 시간증가 폭은 적게 나타나고 있다. 기존의 VPN EDI 데이터 전송방식에서 전송 시간이 늘어나는 것은 데이터는 보안의 방식이 추가되기 때문이다. 따라서 본 연구 EDI Data는 문서를 보안등급에 따라 전송함으로서 비용과 시간의 효율성을 제고하고 있다.



(그림 7) EDI 데이터 전송량과 시간과의 관계



(그림 8) EDI 데이터 전송량과 비용과의 관계

(그림 8)의 경우 Kt-net의 VAN 사용 시 26KB의 경우 표준요금이 기본 20,000원이며 26KB 초과분에 한하여 388원/1KB씩 증대된다. 이는 기업과 은행 간의 데이터의 종류와 관계없이 전송량에 따라 많은 비용이 소요된다. 기존 VAN회선을 사용하는 기업에 비해 본 연구는 ADSL회선 사용비용(KT기준)으로 월정 고정액으로 28,900원의 사용료가 부과된다. 본 연구에 사용된 ADSL 회선의 경우 전송되는 데이터의 양과는 관계없이 일정비용이 소요되고 있다.

EDI 데이터를 중요도에 따라 전송하므로 기존 VAN을 사용하여 전송하는 EDI 데이터에 비해 VPN을 사용하는 EDI 데이터의 전송방식이 비용절감효과를 가질 수 있다.

또한 EDI 데이터를 VPN을 이용하여 데이터를 전송함으로 데이터의 무결성 및 보안, 전송신속성을 가질 수 있다.

즉, 계좌이체 및 비밀번호 등과 같은 중요한 데이터의 문서는 IPSec통신을 이용하여 시간은 다소 소요되지만 보다 안전한 암호화와 인증화 과정을 거치므로 안전한 데이터 전송이 이루어지고 있다.

공중망의 보안성을 VPN을 통하여 획득함으로서 무역 및 은행업무 등 네트워크를 통해서 이루어지는 많은 자료의 공유 및 전송에 관련된 직, 간접적인 비용절감 효과를 기대할 수 있다.

5. 결 론

인터넷은 개방성과 정보 공유라는 강점을 가지고 있는 반면에, 정보의 유출, 파괴, 변조 등의 각종 해킹과 바이러스 침해에 취약한 구조를 가지고 있다. 이에 대한 안전성과 신뢰성을 제공하는 정보 보호 시스템이 인터넷 기반의 정보 인프라 구축의 필수 요소가 되고 있다.

이에 따라 문서와 데이터는 그 중요도에 따라 속도 및 보안의 정도가 결정되어야 한다. 보안에 철저해야 하는 문서는 데이터의 전송속도를 무조건 빠르게 전송하기보다 보안에 치중하여야 한다.

또한 전송속도를 빠르게 처리해야 하는 문서인 경우 보안적인 면보다는 속도를 우선적으로 처리하여야 할 것이다.

따라서 전송속도 및 보안은 상황에 따라 꼭 필요한 부분의 네트워크 정보를 적절히 사용한다면 보다 효율적이다.

이에 EDI 시스템에서 VPN장비로 상황에 따라 적절히 접속하여 보안에 관련된 정책 등을 효율적으로 처리함으로서 처리속도와 보안에서 개선될 수 있다.

참 고 문 헌

[1] Wilson Company, "EAI extends EDI systems", InfoWorld, Vol.24, No.47, 2002.

[2] 한국정보보호진흥원 "정보보호 산업의 현황과 발전방향", 한국정보보호진흥원 제6호 정보통신 심포지움, 2001.

[3] 양창욱, "www환경에서의 c4I체계 상호운영성을 위한 정보보호체계 구축방안", pp.35~38, 한남대학교 대학원 석사학위논문, 2002.

[4] Nicolas P., "Secure group management : Secure long term communities in ad hoc networks", Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003.

[5] Christian H., "Unambiguous access to XML-based business documents in B2B e-commerce", Proceedings of the 3rd ACM conference on EC, 2001.

[6] Korhonen R. and Salminen A., "Visualization of EDI messages : facing the problems in the use of XML", ACM Press, 2003.

[7] Karen K., John W., and Vicki H., "The EDI implementation decision : a small business perspective", ACM Press, 1997.

[8] Turban E., "Introduction to E-Commerce", Prentice Hall, pp.273~280, August, 2002.

[9] 표성배, "적응제어 IPSec과 전자서명을 이용한 안전한 XML문서 교환시스템의 설계 및 안전성검증", 숭실대학교 대학원 박사학위논문, 2003.

[10] 고영중, 서정연, "문서관리를 위한 자동문서 범주화에 대한 이론 및 기법", 정보관리연구학회 Vol.33, No.2, pp.19-32, 2002.

[11] 한국정보보호진흥원 "정보보호 관리통제", 한국정보보호진흥원.

[12] 국가행정 연구원 "[일본] 개인정보보호법 관련 기업 지침 공표", 니혼게자이, 2003.

[13] 백유미 "국내 수출기업의 웹기반 물류 EDI 도입요인 및 성과에 관한 실증 연구", 2004, 한남대학교 대학원 박사학위논문, 2004.

[14] K. Muthukrishnan, "A core MPLS IP VPN architecture", Work in progress, RFC 2917, July, 2001.

[15] Townsley, A, Valencia, A, Rubens, G, Pall, G, Zorn, and Palter, "Layer Two Tunneling Protocol L2TP", Network Working Group, RFC2661, August, 1999.

[16] Kaufman C., Periman R., and Sommerfeld B., "Dos Protection for UDP-Based Protocols", Proceedings of the 10th ACM conference on Computer and communications security, 2003.

[17] 강문희, 정명태, "VPN 기술의 개요", 통신정보보호학회학회지, 제9권 제4호, 1999.

[18] Nachiketh R. Potlapally "Power modeling and optimization for embedded systems : Analyzing the energy consumption of security protocols T", Princeton University, August, 2003.

[19] 윤재우, 이승형, "IP 기반 VPN 프로토콜의 연구동향 확장성과 보안성", 한국정보보호학회 학술저널, Vol.11, No.6, 2001.

[20] 시장보고서, "VPNs Take a New Look : Trends in the US IP VPN Services Market", Instat/MDR, 2004.

[21] 이계상, "정보통신 및 표준기술동향", TTA저널, 2002.

약어표기

EDI : Electronic Data Interchange
VPN : Virtual Private Network
VAN : Value Aided Network
공용 인증망 : Public Switched Network
SA : Security Association
AH : Authentication Header

ESP, Encapsulated Security Payload
L2TP : Layer Two Tunneling Protocol
PPP : Point-to-Point Protocol
ECP : Encryption Control Protocol
CCP : Compression Control Protocol
TACACS : Terminal Access Controller Access Control System
RADIUS : Remote Authentication in Dial-Up User Service
PAP : Password Authentication Procedure
CHAP : Challenge-Handshake Authentication Protocol : CHAP
IPSec : Internet Protocol Security
ICV : Integrity Check Value
MAC : Message Authentication Code
SPI : Security Parameters Index
ISAKMP : Internet Security Association and Key Management Protocol
NAT : Network Address Translation
IKE : Internet Key Exchabge
DOI : Domain Of Interpretation

최 병 훈

e-mail : choihuni@naver.com
2001년 성결대학교 전산통계학과(학사)
2004년 숭실대학교 산업기술정보대학원 산업정보시스템공학과(석사)
2000년~2003년 (주)다일웹정보 C/S 기술팀
2003년~현재 시소닷넷 보안사업부
관심분야 : EDI, VPN, IPSec, L2TP, 정보보안

이 건 호

e-mail : ghlee@ssu.ac.kr
1986년 대구대학교 산업공학과(학사)
1991년 인하대학교 산업공학과(석사)
1996년 U. of Iowa, Dept. of Industrial Eng.
1997년~1999년 숭실대학교 산업공학과 전임강사
1999년~2004년 숭실대학교 산업·정보시스템공학과 조교수
2004년~현재 숭실대학교 산업·정보시스템공학과 부교수
관심분야 : OOD, 정보보안, E-business, AI, Manufacturing System, Product Design