情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

Smart Grid를 위한 필드형 가상사설망(VPN) 게이트웨이의 구현

박 준 영,† 김 휘 강‡
고려대학교, 정보보호대학원

A Study on the Implementation of outdoor type Virtual Private Network Gateway for Smart Grid

Jun Young Park,† Huy Kang Kim‡
Korea University, Graduate School of Information Security

요 약

우리나라의 전력분야 제어시스템은 보안에 우수한 폐쇄형 네트워크로 운영되고 있어 보안피해의 심각성을 대체로 인지하지 못하고 있다. 앞으로 스마트그리드 사업이 지속적으로 확대되면 스마트미터에서부터 발전소에 이르기까지 다양한 형태의 사이버공격이 이루어질 수 있다. 향후 스마트미터를 통해 발전소에서 가정집까지의 전체 전력망이 연결되면 보안은 더욱 중요한 요소가 될 것이다. 본 연구에서는 스마트그리드 환경 즉, 외부의 혹독한 환경과 전국적인 망에서의 안정적 데이터 전송과 외부로부터의 침입방지를 위해 필요한 가상사설망(VPN) Gateway 구조를 설계 및 구현하였다. 본 연구를 통해 완성된 시제품으로 기 운영 중인 상용제품과 다양한 방식으로 연동 테스트를 시행하였으며, IPSec 방식의 터널링과 ARIA 암호화 알고리즘을 통한 암호화를 통해 전력선통신(PLC) 저압원격검침 분야에 시범 설치되어 보안이 강화된 데이터통신을 하고 있다.

ABSTRACT

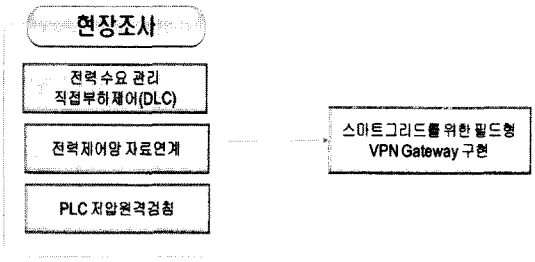
The vulnerabilities existed in Korean electricity control systems is unexposed because it is being operated in a closed network with superior security. The threat will become greater once the closed network develops into a smart grid environment with superior intelligence. Security will have a greater impact once each household will be connected to the power plant via the smart meter. This research focuses on stable data transfer in harsh external environment and whole-nation coverage network, and suggested standardized and optimized Virtual Private Network (VPN) Gateway architecture to support Power Line Communication (PLC). The functionality and stability of the prototype has been verified with field tests. For implementation of outdoor type VPN device for smart grid, we adopted PLC low voltage remote-meter-net for data communication. Also, IPSec type tunneling and ARIA algorithm based encryption of data collected by PLC low voltage remote meter is transmitted.

Keywords: SmartGrid, VPN Gateway, IPSec, PLC, Security

I. 서 론

본 연구는 스마트그리드 환경에 적합한 필드형 가상사설망(VPN, Virtual Private Network) Gateway를 설계 및 구현하는 것으로 현재 다양한 형태로 운영되고 있는 PLC(Power Line Communication, 전력선통신), DLC(Data Link Control, 데이터링크제어), SCADA(Supervisory Control And Data Acquisition, 원격감시제어) 운영 현황

접수일(2011년 5월 20일), 게재확정일(2011년 7월 29일)
† 주저자, kepcopjy@kepco.co.kr
‡ 교신저자, cenda@korea.ac.kr



〔그림 1〕 연구내용

조사를 통해 옥내/옥외 철구함 안에 VPN Gateway가 설치 가능하도록 경량화하고 VPN의 핵심 기능만 탑재하여 광범위한 스마트그리드 환경에서 비용 대비 효과를 극대화하여 혹독한 환경(온·습도, 진동, 크기, 저속) 속에서 안정적인 동작을 구현하는데 있다.

현재 시중에 판매되는 VPN Gateway는 다수의 사용자가 동시에 사용하는 OA(Office Automation) 용도로 개발되어 많은 기능과 고비용이 요구된다. 스마트그리드 환경에 맞는 필드형 VPN Gateway는 설치 장소가 옥외 스위치 야드, 전주 위 등으로 온·습도, 진동 및 크기 등에 취약하며, 검침데이터 전송용으로 소용량의 데이터 통신을 요구한다. 아래 〔그림 1〕은 연구개발 내용에 대한 요약이다.

II. 관련연구

기존의 전력망(Grid)에 지능형기술(Smart)을 접목하여, 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형전력망이라는 의미의 스마트그리드와 공중통신망을 이용하여 가상의 전용 사설망 기능을 부여하는 서비스인 VPN 서비스를 이해하는 것이 중요하다.

2.1 스마트그리드

스마트그리드는 양방향 전력 정보 교환을 통하여 합리적 에너지 소비를 유도하고, 고품질의 에너지 및 다양한 부가서비스를 제공한다. 또한 신재생 에너지, 전기차 등 청정 녹색 기술의 접목·확장이 용이한 개방형 시스템으로 산업간 융·복합을 통한 신 비즈니스 창출이 가능하다〔1〕.

2.2.1 VPN

인터넷은 전 세계적으로 급격히 확산되어 편리하게 사용되고 있으나, 개방성과 확장성으로 인한 취약성 노출, 해킹 등으로 인한 정보의 유출, 변조 및 도용 등의 역기능이 발생하고 있다. 또한 속도 저하 등의 서비스의 질을 향상시키기 위한 전용망의 설치는 인터넷에 비해 안정적이나 고비용을 수반하는 전용 네트워크 구축이라는 단점이 있다. 이런 기존의 인터넷과 전용망의 한계를 효과적으로 극복할 수 있는 방법으로 주목받고 있는 서비스 중의 하나가 VPN 기술이다. 즉, VPN 이란 공중망(ADSL, VDSL, 케이블모뎀 등) 위에 특정한 개인이나 회사만 이용할 수 있는 암호화된 통신채널을 한 번 더 구축하는 것을 말한다.

2.2.2 VPN의 핵심기술

VPN의 핵심기술은 크게 터널링 및 암호화 기술로 나눌 수 있다. 터널링(tunneling)이란 시작 지점에서 목표 지점까지 터널을 형성한다는 의미로서 인터넷에서 네트워크상에서 외부의 영향을 받지 않는 가상적인 터널을 형성하여 정보를 주고받는다는 개념이다. 이를 구체적으로 설명하면 네트워크상의 터널과 관련된 상호 약속된 프로토콜로 세션을 구성하고 이 터널을 다른 사용자로부터 보호를 받는다는 것이다. 이러한 터널링을 위한 프로토콜은 OSI기준 계층별로 여러 가지가 있는데 네트워크 계층의 IPSec(IP Security Protocol)을 널리 사용하고 있다. IPSec은 AH(Authentication Header)와 ESP(Encapsulation

〔표 1〕 주요 VPN 프로토콜 비교

구 분	PPTP	L2TP	IPSec
표 준 화	Microsoft	RFC 2661	RFC 2401~2410
제공계층	OSI 2계층	OSI 2계층	OSI 3계층
모 드	client-server	client-server	peer-to-peer
제 공 프로토콜	IP, IPX, NetBEUI, etc	IP, IPX, NetBEUI, etc	IP
터널서비스	single PPP tunnel per connection	multiple PPP tunnel per connection	multiple PPP tunnel per SA
데이터인증 및 암호화	× (ppp제공)	× (ppp제공)	Packet단위제공
키 관 리	×	×	ISAKMP/IKE
엑세스제어	×	×	packet filtering

Security Payload) 등의 프로토콜로 구성되어 있으며, AH 프로토콜은 데이터의 무결성과 근원지 IP 인증 및 재사용을 방지하기 위해 캡슐화를 이용하여 침입자의 공격에 대항한 방어책을 제공하는 방법으로 인터넷에서의 보안 문제인 인증, 무결성, 기밀성 및 리플레이 공격 방지 등을 제공하기 위해서 만들어진 것으로서 VPN 터널링을 위한 보안 서비스 제공에 적합하다[10][11][12].

암호화는 통신되는 데이터를 암호화해 전송하는 것으로 사전에 약속된 키(Pre-shared key)로 암호를 해독하는 사용자를 제외한 어느 누구도 데이터를 볼 수 없게 하기 위한 기술이다. 암호화는 IPSec의 구성요소 중 기밀성과 무결성을 제공하는 ESP (Encapsulation Security Payload)에서 주로 하게 되는데 암호화 방식은 DES와 3DES 암호화 알고리즘이 사용되며 이를 통해 해커의 침입이나 타 네트워크의 사용자들이 데이터의 내용을 분석할 수 없게 하는 기능을 제공한다. 데이터를 안전하게 보관 및 전송하기 위한 암호화 기술로 보안영역 및 폴더, 파일의 암호화 알고리즘은 국가 표준 암호화 알고리즘 SEED, ARIA를 수용하고 있으며, SEED는 1999년 9월 한국정보통신기술협회(TTA)으로 제정되었으며, 2005년에는 국제 표준화 기구인 ISO/ IEC 국제 블록암호 알고리즘 표준으로 제정되었으며, 같은 해 IETF 표준으로도 제정되어 있다[13].

2.3 스마트그리드 보안환경

정보통신의 발달로 다양한 송변전 원격감시제어시스템(SCADA), 배전자동화시스템(DAS, Distribution Automation System), 원격검침시스템(AMR, Automatic Meter Reading), 직접부하제어시스템(DLC, Data Link Control) 등이 증가하였다. 또한 국가 간, 기업 간 경쟁의 격화 및 각종 규제 완화로 원격감시제어시스템의 기능 및 역할의 변화가 초래되었다. 즉, 원격감시제어시스템간의 상호 연동 및 외부 경영시스템으로 데이터를 제공하기 위한 연계점이 증가하여 시스템 간 신뢰성 확보가 중요한 요소로 등장하였으며, 폐쇄형 구조에서 상용 운영체제(OS) 사용 등 개방형 시스템으로 전환되었다[3].

통신시스템도 산업 표준인 TCP/IP 방식으로 전환되어 어디에서라도 자유로운 접근이 가능해졌다. 그러나 이러한 원격감시제어시스템은 개발 및 구축 당시 보안을 고려하지 않고 개발된 시스템으로 보안 기능의 요구에 대응하기에는 어려움이 있다. 이에 따라 보안 기준을 만족시키기 위해 추가적인 처리 능력 향상과 통신 대역폭 확장 요구, 보안 기능 추가 등의 방안이 필요하다.

2.3.1 스마트그리드 보안문제

전력 인프라의 보안 문제는 수년 동안 계속해서 제기되었다. 시장분석 기관 가트너(Gartner)는 2004년에 핵심 인프라에 IP 네트워크를 사용하는 것은 해커들의 사이버 공격 대상이 될 수 있다고 경고한 내용을 발표하였다. 즉, 인터넷으로 대변되는 IP 네트워크를 사용하게 됨으로써 언제 어디서나 핵심 인프라에 접근이 가능하게 되는 것이다. 2008 RSA conference에서는 전력업체 직원이 일반인이 흔히 사용하는 이메일 서비스를 이용하다가 멀웨어를 자신의 컴퓨터에 다운로드하게 되고, 나아가 발전소 전체를 마비시키는 과정을 시현했었고, 2009년 BlackHat USA 2009에서는 전기신호로 메모리 데이터를 조작하여 스마트미터(smart meter)를 제어하는 과정을 시현했었다[2].

전력 인프라에 보안에 대한 경고는 현재까지 계속해서 발생하고 있다. 미국 보안전문 회사 IOActive (2009.03)는 자사의 연구결과를 바탕으로 스마트그리드 플랫폼에 커다란 보안 결함이 존재한다고 보도하였다[5]. IOActive는 스마트그리드가 프로토콜 변경, 버퍼오버플로우(Buffer Overflow), 루트킷(root-kit) 코드 증식과 같은 일반적인 보안 취약점들에 노출되어 있다고 주장하였다. 실제 전력 분야에 대한 해커들에 의한 침입의 예는 다음과 같다. 월스트리트 저널(2009.4.8)은 미국의 국가 전력망이 외국 해커들에 의해 침입 당했다고 보도하였다. 중국, 러시아의 해커들이 미국의 전력망 시스템에 침투해 전력 제어망을 교란시키는데 활용되는 소프트웨어를 심어놨다고 보도하였다. 월스트리트 저널은 미국 보안당국 관계자의 말을 인용해 그 침투를 전쟁과 같은 비상시에 미국 전력망에 침투해 주요 인프라의 활성화를 차단하려는 사이버스파이의 훈련으로 추정하였다. 한편 2008년 1월 CIA가 미국 특정 지역의 여러 도시의 정전이 해커들에 의해 일어났음을 확인하였고, NSA(National Security Agency : 미국국가안전보장국)의 전 직원이자 전력 네트워크의 공격 시뮬레이션 전문가는 수년 동안 전력 제어망에 해커가 침투하였다고 밝혔다[2].

폐쇄망에서 개방형 스마트그리드 환경으로 진화하

면서 네트워크 간 연동 및 IP 네트워크로 전환이 되기에 보안 위협은 더 커지고 있는 실정이다. 또한 각 가정마다 스마트 미터를 통해 발전소에서부터 가정집까지의 전체 전력망 전체가 연결이 되기에 보안은 더욱 더 중요하게 된다[4].

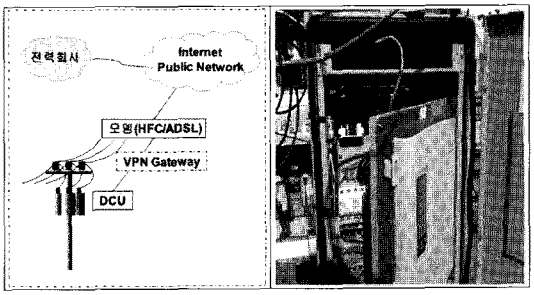
2.3.2 데이터 신뢰성

스마트그리드 환경의 IP 네트워크로 연결된 신뢰할 수 없는 통신경로를 지날 때 발생하는 데이터의 위·변조, 정보 유출, 서비스 거부 공격(Denial of Service Attack) 및 경로 변경 공격(Routing Attack) 등에 대비하여 암호화된 통신이 가능한 안전한 통신 채널 확보가 필요하다. 또한 원격지의 제어시스템 및 각 메시지의 정확한 식별 및 인증이 없을 경우 시스템의 건전성 보장이 어려워 제어시스템의 총체적인 붕괴를 초래할 수 있다.

그러나 제어시스템에 암호화 및 인증 기능 등 보안 기능을 추가로 요구 시 시스템의 한계 및 호환성 확보, 안정성 저해 등 시스템의 문제를 초래할 수도 있다. 따라서 암호화, 인증 등 문제를 해결하기 위해 TCP/IP 네트워크에서 표준화된 IPSec 방식의 VPN을 이용하는 것이 타당하다. 앞의 [표 1]에서 보는 바와 같이 2계층 프로토콜인 L2TP 등에 비해 3계층 프로토콜인 IPSec이 IP 계층에서 암호화하여 보안성을 향상시켜준다. IPSec 방식은 PPP에 의해 제공되는 데이터 인증 및 암호화를 Packet 단위로 할 수 있기에 국제표준 VPN 프로토콜로써 널리 사용된다. 상용제품도 IPSec 기반 터널링을 제공하기에 스마트그리드를 위한 필드형 VPN Gateway도 IPSec을 지원하도록 한다[11][12].

[표 2] VPN Gateway 상용제품 운영환경

상용제품 개발회사	제품명	운영환경
넥스지	VForce860	정보 없음
시큐아이닷컴	NXG100V	온도 : 5~40℃ 습도 : 20~90%
시스코	Absolute 100	정보 없음
안철수연구소	ezWall v3.0	온도 : 0~50℃
어울림정보기술	soligate VPN	정보 없음
인프니스	secuwaygate100	온도 : -15~50℃ 습도 : 5~90%
퓨처시스템	xecurevpn 1000	온도 : 0~40℃ 습도 : 10~90%



[그림 2] 필드형 VPN Gateway - 옥외 전주 설치 위치

2.3.3 혹독한 외부환경 및 전국적 분포

[표 2]와 같이 현재 시중에 판매되는 상용제품인 VPN Gateway는 다수의 사용자가 동시에 사용하는 OA(Office Automation)용도로 개발되어 많은 기능과 고비용이 요구된다. 스마트그리드를 위한 VPN Gateway는 설치 장소가 옥외 스위치 야드, 전주 위 등으로 온·습도, 진동, 크기 등으로 매우 열악하다. 스마트그리드 환경에서 안전한 데이터 전송을 통신채널 확보를 위해 VPN Gateway를 사용하려면 우선적으로 크기도 문제지만, 실제 운영 환경에 대한 고려가 가장 중요하다.

스마트그리드를 위한 VPN Gateway 설치 장소는 아래 [그림 2]와 같이 옥외의 기존 데이터수집장치(DCU, Data Concentration Unit)와 데이터 통신용 모뎀 사이에 VPN Gateway를 설치하여야 한다[8].

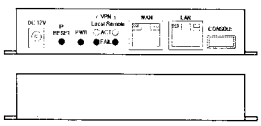
III. 필드형 VPN Gateway 설계

스마트그리드 환경에 적합한 필드형 VPN Gateway 구현을 위해 현재 다양한 형태로 운영되고 있는 PLC, DLC 및 SCADA 운영 현장의 환경 조사를 통해 옥내/외 철구함 안에 설치 가능하도록 경량화하고, 핵심 기능만 탑재하여 광범위한 스마트그리드 환경에서 비용 대비 효과를 극대화하여 옥외 전주 위 등의 혹독한 환경 속에서 안정적인 동작이 가능하도록 설계하였고, 시작품으로 실제 운영 중인 PLC 저압 원격검침망에 시범 적용을 하였다. 또한 추가개선 사항을 도출하여 최종 제품에 반영하였다.

3.1 스마트 그리드 환경에 적합한 요구사항

현장 실사 및 기 상용제품 자료 조사를 통해 아래

〔표 3〕 주요 요구사항 요약

요구사항	개발사항
다량으로 필드에 설치	온/습도 한계치 상승, telnet 등 원격 접속 지원
다량의 VPN Gateway 원격 감시제어	관리시스템과 연동을 위해 SNMP agent 개발 지원
온도, 습도는 한국산업규격 KS C를 반영	온도 -20도에서 70도까지, 습도 90%까지 안정적 동작 지원
ADSL 모뎀 등 확장성	ADSL, cable modem 지원
상용제품과 호환	상용제품과 호환 지원
VPN 정상동작 여부 표시	VPN Remote(Local) LED : - 터널 미 생성 : 비 점등 - 정상 : 녹색 - 비정상 : 적색, Gateway 무응답(비정상) 시
운영 효율성 향상 (LED와 포트 동일위치)	
국정원 인증 암호 알고리즘 구현	ARIA 암호 알고리즘 적용 (Key size 128, 192, 256 bit)
DHCP server 기능구현	DCU 장비 하단에 연결되는 slave DCU에 대한 IP 부여를 위해 DHCP server 기능 지원
IP layer DF flag 강제 조정 구현	DCU에서 전송되는 검침데이터의 IP packet내에 DF flag 설정값의 유/무와 상관없이 VPN Gateway에서 데이터를 1.500 byte로 Fragment해서 전송토록 지원

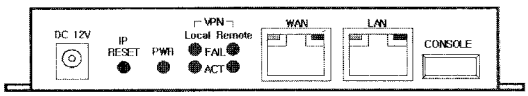
〔표 3〕과 같은 스마트그리드 환경에 적합한 요구사항을 받아 개발하였고, 시범 사업을 통해 실 환경에 최적화되게 사용할 수 있도록 기능을 추가하였다.

3.2 H/W 개발 규격

국내에서 많이 사용되는 상용제품의 경우 VPN Gateway의 스펙은 VPN 기능 외에 침입차단시스템 및 이중화 기능이 포함된 고성능 제품이다. 스마트그리드를 위한 VPN Gateway는 설치 장소가 옥외 스위치 야드, 전주 위 등으로 온·습도, 진동 및 크기 등 열악하다. 따라서 전력 IT환경에 적합하게 설치 적용되도록 설계되고, 관리 특성에 맞게 VPN의 핵심기능만 탑재시켜 기능이 단순하면서 상대적으로 저가인 필드형 VPN Gateway 개발이 필요하다.

〔표 4〕 VPN Gateway 하드웨어 사양

항 목		내 용
하드웨어	CPU	Arm940t (166Mhz 32bit-RISC)
	Memory	64MB (SDRAM)
	Flash	16MB
	Network	RJ-45 2Ports E/A (10/100 Base T)
	LEDs	Red 2 E/A, Green 3 E/A
	전 원	Input : AC 110~220V, 60Hz, Output : DC 12V/1.0A, 10W
	크 기	135 x 96 x 25 mm
	운용환경	온도 : -20℃~70℃, 습도: 5~90%



〔그림 3〕 하드웨어 전면

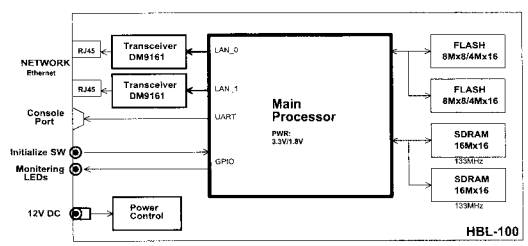
전력 IT 환경에 최적화된 VPN Gateway 개발을 위해 embedded 전용 Linux를 사용하며, 최소화된 입/출력 × 2 포트로 구성되며, 옥내/외 철구함 내부에 설치가 되도록 크기를 줄였으며, 실외에서도 동작이 가능하도록 동작 가능한 온도를 OA용 보다 높였다.

3.2.1 하드웨어

하드웨어의 특징은 운영자 확인을 편리하게 하기 위해 LED와 포트 위치를 동일하게 한 점이다. 그리고 하드웨어 외형은 전지적 노이즈의 차폐 특성과 방열 특성이 우수한 알루미늄 재질로 제작하였으며 제품 설치 시 고정을 위한 고정 홈을 만들었다.

3.2.2 Prototype 회로도면

회로의 구성은 프로세서를 중심으로 OS와 응용프로그램이 저장되는 Flash Memory, 프로세서의 연



〔그림 4〕 블록도

산과 응용프로그램의 수행에 필요한 임시 저장 공간인 SDRAM이 연결되고, 두 개의 Ethernet 인터페이스를 사용할 수 있도록 하는 LAN 송수신용 칩이 연결되며, 프로세서에 직접 명령어를 입출력할 수 있는 직렬 통신포트와 시스템의 동작 상태를 표출하는 LED 및 시스템의 전원을 공급하는 전원장치로 구성된다.

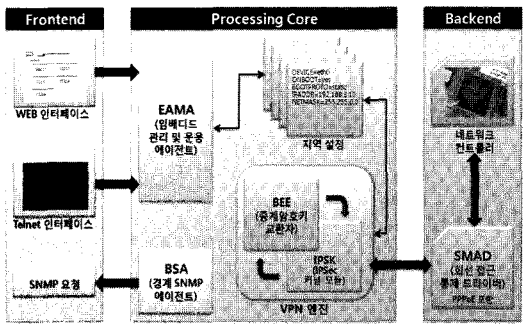
3.3 S/W 개발 규격

상용제품 VPN Gateway는 다수의 사용자가 동시에 사용하는 OA용도로 개발되어 많은 기능과 고비용이 요구된다. 부가적인 침입차단시스템 기능, 이중화 기능 및 유해사이트 차단 기능 등이 있다. 앞서 열거한 기능 중 이중화의 경우, 예기치 않은 사고로 인해 하나의 시스템에 장애가 발생하더라도 다른 시스템이 이를 감지하고 역할을 대행하는 기능으로 스마트그리드를 위한 필드형 VPN Gateway에서는 반드시 필요한 기능이 아니다. 또한 유해사이트 차단 기능 또한 검침 데이터를 주고받는 게 전부인 스마트그리드 환경에서는 불필요한 기능이다.

스마트그리드 환경에 최적화된 VPN Gateway 구현을 위해 OA용으로 개발된 상용제품이 기본적으로 제공하는 침입차단시스템 및 이중화 기능을 축소하였으며, 상용제품 VPN Gateway와 호환되며 PLC 및 DLC 환경에 적합하도록 ADSL 및 cable modem을 지원하도록 설계하였다.

〔표 5〕 VPN Gateway 소프트웨어 사양

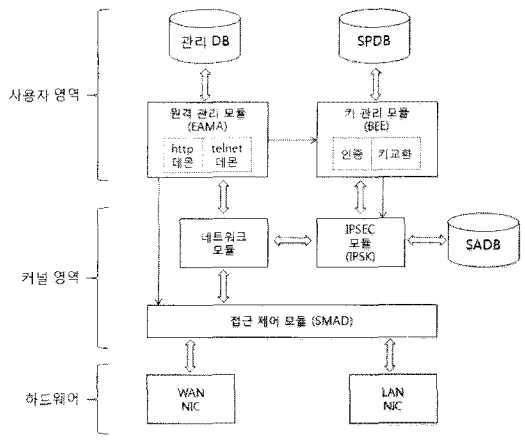
항 목			내 용
소프트웨어	OS	OS	μcLinux GNU/Linux (Kernel 2.4.17 with uC-pre5)
		Compile 환경	gcc 2.95.3 (arm-linux cross compiled)
	운용관리	Console 관리	Serial-port를 통한 긴급 복구 및 초기 설정
		Telnet관리	RFC 854 준수, 원격 Console 설정 모드
		Web관리	RFC 2068 준수, 원격 GUI 설정 모드
		Firmware	TFTP로 자동 업그레이드, Web으로 수동 업그레이드
소프트웨어	네트워크	IP설정	Static IP, Dynamic IP (DHCP)
		라우팅	Static Routing, RIP v1/v2
	IPSec VPN	헤더	ESP, AH
		인증	MD5, SHA1, SHA2
		암호화	DES, 3DES, AES, ARIA



〔그림 5〕 VPN Gateway S/W 구성도

3.3.1 VPN Gateway S/W 구성도

VPN Gateway 모듈은 〔그림 5〕과 같이 크게 3가지 (front-end, processing core, back-end)로 나뉘며, 다음의 역할을 한다. Front-end는 사용자 레벨로써, UI(User Interface)와 같은 사용자 입출력을 처리하는 모듈들이 여기에 있으며, 주로 운용자가 접하는 부분이다. Processing core는 운영체제 레벨로써, 실제로 VPN이 동작하는데 있어 관리, 작동 통제 및 감시를 처리하는 영역이다. Back-end는 드라이버 레벨로써, 주로 네트워크를 제어하며 H/W 및 네트워크 환경의 영향을 많이 받는다.



〔그림 6〕 시스템 상세 구성도

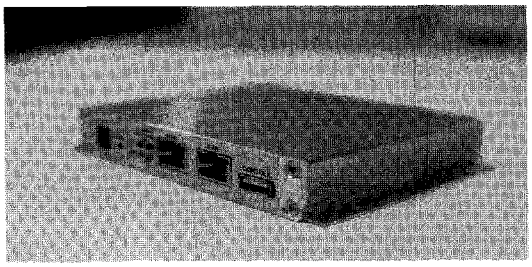
3.3.2 기능 설계

VPN Gateway는 네트워크 연결의 보안을 준수하기 위하여 RFC 1825 및 RFC 1829에 정의되어 있는 IPSec 기능을 제공하며, 하드웨어 부분과 커널 영역 부분 및 사용자 영역으로 나누어져 있는 구성이다.

하드웨어 부분은 네트워크 인터페이스 카드(NIC)로 일반적으로 public 영역과 연결되는 WAN NIC (Network Interface Card)와 private 영역과 연결되는 LAN NIC가 있다. WAN NIC는 다른 Gateway나 클라이언트와 터널링을 통해 암호화된 상태의 패킷을 송수신하며 LAN NIC는 복호화된 상태의 패킷을 송수신 한다.

접근 제어 모듈은 NIC를 통해서 들어오고 나가는 패킷에 대하여 설정된 접근 제어 규칙에 의해서 필터링을 하게 된다. 접근 제어 규칙은 매니저에 의해서 설정을 하게 되는데, 원격 관리모듈을 통해서 명령이 전달되게 된다. 네트워크 모듈은 TCP/IP를 포함하는 모든 네트워크 패킷에 대한 처리를 하게 되며, IPSec 모듈은 IPSec 패킷에 대한 처리를 담당한다. SADB (Security Association Data Base)는 키 관리 모듈에 의해서 생성된 SA 정보가 IPSec 모듈을 통해서 커널 영역 메모리에 저장을 한다. SADB에는 인증키, 암/복호화 키 및 SPI 등이 저장되어 있다. IPSec 모듈이 암/복호화 과정에 필요한 키를 얻는 데에 사용된다.

사용자 영역의 키 관리 모듈은 인증, 키 교환, CA 서버 연동의 기능을 담당하며, 키 교환 프로토콜인 IKE를 담당하는 데몬을 포함하고 있다. UDP 포트 500번을 통해서 상대편 Gateway나 클라이언트와 IKE 프로토콜에 의한 키 교환을 한다. 이렇게 생성된 키와 관련한 정보는 IPSec 모듈에 전달하여 암/복호화 과정에 사용이 된다. CA 서버에서 인증서를 받아 자체 인증에 사용하는 것도 여기서 담당한다. 이 밖에도 여러 보안 정책을 저장하고 있는 SPDB를 관리하기도 한다. SPDB(Security Policy Data Base)는 인증(authentication)과 암호화(encryption)의 방법에는 다양한 방법이 존재하게 된다. 이러한 여러 방법 중 적당한 선택을 통해 보안 정책이 결정되게 되는데, 이러한 정보를 담고 있는 것이 SPDB이다. DB라 하여 파일 등의 형태로 따로 존재하지는 않고, 키 관리 모듈의 일부로서 메모리에 존재하게 된다.



〔그림 7〕 완성된 VPN Gateway 사진

IV. 필드형 VPN Gateway 구현

하드웨어는 필드형 VPN Gateway에 적합하도록 산업 기준에 따라 고온 다습한 환경을 고려하여 설계하였고 그에 부합되는 부품을 사용하였다. 기 상용제품과 달리 필드형 VPN Gateway는 관리의 편의를 위해 LED와 포트 위치를 동일하게 배치하였으며, VPN 관련 동작 상태를 별도로 파악하기 위해 추가 LED를 구현하였다. 또한 폐쇄된 사내 네트워크와 지역 사설 네트워크를 연결하기 위한 VPN 기능을 제공하며 VPN 기능은 국제표준인 IPSec으로 구성된다.

4.1 보안기능

4.1.1 대칭키 알고리즘

검침 데이터의 위·변조를 방지하기 위해서는 적절한 보안 기능이 필수이다. 필드형 VPN Gateway의 보안 기능 분석은 다음과 같다. 〔표 6〕에서와 같이 IPSec 패킷 암호화를 위해 대칭키 알고리즘을 사용하고, 제공되는 암호 알고리즘은 DES, 3DES, AES 및 ARIA이며 사용모드는 CBC(Cipher Block Chaining)이다.

키의 길이는 IKE 단계에서 IPSec 단말 노드끼리 협상하는 키 길이를 이용하며 DES의 경우 블록 크기를 64bit, 3DES의 경우 블록 크기를 192bit,

〔표 6〕 VPN Gateway에서 사용하는 대칭키 알고리즘

알고리즘	키(블록)길이	모드	출처	목적
DES	56bit(64bit)	CBC	LGPL/ OpenSSL (libcrypt)	IPSec 패킷 암호화
3DES	168bit(64bit)			
AES (Rijndael)	128, 192, 256bit (128, 192, 256bit)			
ARIA	128, 192, 256bit		국가정보원	

AES 및 ARIA의 경우 블록 크기를 128, 192, 256bit로 하여 협상할 수 있다. IKE 단계에서 단말 노드끼리 키를 협상하고 나면, 해당 키는 협상에 따라 최소 1,200초에서 최대 3,600초까지 메모리에 적재하며, 키가 만료되기 전에 새로운 키를 협상한다. 즉, 위의 알고리즘에 사용하는 키는 장비에 보관하지 않는다.

IPSec 표준(RFC2401)에 따르면 IPSec은 기본적으로 3DES를 지원하여야 하며, AES를 추가로 권장하고 있다. 본 제품에서 DES는 하위 버전 호환성을 위해 지원하고 있으며 IKE 협상은 보안 등급이 가장 높은 AES-256bit를 기본으로 지원하고 있다[10].

4.1.2 비대칭키 알고리즘

사용하는 알고리즘의 종류는 [표 7]과 같다.

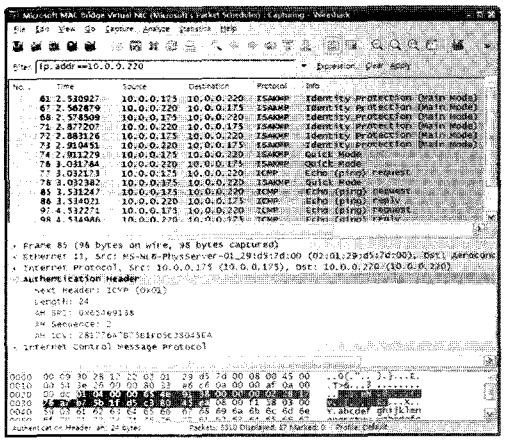
[표 7] VPN Gateway에서 사용하는 비대칭키 알고리즘

알고리즘	출처	사용목적
MD5	LGPL/ OpenSSL (libcrypt)	- IPSec 패킷 무결성 검증 - 사용자 계정/비밀번호 암호화
SHA-1		- 상 동 - IKE 협상 시 VPN Gateway 인증하기 위한 공유키

위의 알고리즘은 시스템에서 메시지를 해시하여 사용하므로 암호화는 가능하나 복호화가 불가능하다. 또한 사용 목적에 따라 해시의 길이가 다르므로 결과값의 크기가 달라진다. 알고리즘에 따른 결과 크기 및 보관 방법은 [표 8]와 같다. IPSec의 무결성 검증 용도로 사용되는 해시의 결과는 HMAC(Header Message Authentication Code) 방식으로 상위 96bit를 잘라서 사용하기 때문에 결과 크기가 항상 96bit로 동일하다.

[표 8] 비대칭키 알고리즘의 용도에 따른 결과

알고리즘	용도	결과 크기
MD5	사용자 계정 해시	176bit
SHA1	사용자 계정 해시	344bit
SHA1	IKE 공유키	344bit
MD5	IPSec 무결성 검증	96bit
SHA1	IPSec 무결성 검증	96bit



[그림 8] AH 헤더를 이용한 IPSec 통신

4.1.3 보안기능 구현

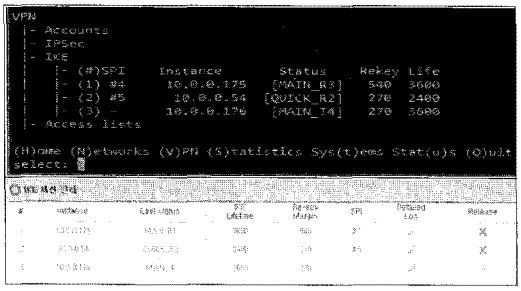
필드형 VPN Gateway에서 AH(Authentication Header) 헤더를 이용하여 IPSec 통신을 하는 화면은 다음의 [그림 8]와 같다. ISAKMP 프로토콜은 IPSec 협상 과정에서 Key 및 알고리즘을 협상하는 과정을 의미하며, 협상이 진행된 이후에 전달되는 패킷들은 AH를 이용하여 인증이 됨을 알 수 있다. AH가 적용된 IP 패킷은 인증만을 하고 패킷 암호화는 처리되지 않으며, 아래의 패킷 캡쳐 프로그램에서 관련 내용을 확인할 수 있다.

4.2 VPN 게이트웨이 관리기능

4.2.1 구성관리

장비의 설정을 위해 세 가지 방식이 가능하도록 구현하였다. 첫째 Console 연결, 둘째 Telnet 연결, 셋째 HTTP 연결로 수행이 가능하다. VPN Gateway에는 WAN과 LAN의 두 가지 네트워크 인터페이스가 유효하며, WAN은 외부망으로 접속되고 LAN은 내부망에 접속되도록 구현되었다. WAN 설정방식은 static IP 설정, DHCP 설정, PPPoE 설정이 가능하다. 또한 장비 관리를 위해 장비에 어떤 문제가 생겼을 경우, NMS(Network Management System)로 통보(Trap)를 할 수 있게끔 하는 서비스가 가능하도록 통보 설정이 가능하다.

터널 설정 메뉴에서는 IPSec 터널을 설정할 수 있으며, 설정된 터널은 IPSec 표준에 의하여 주기적인 키 갱신이 이루어진다. 터널 설정을 위해서는 기



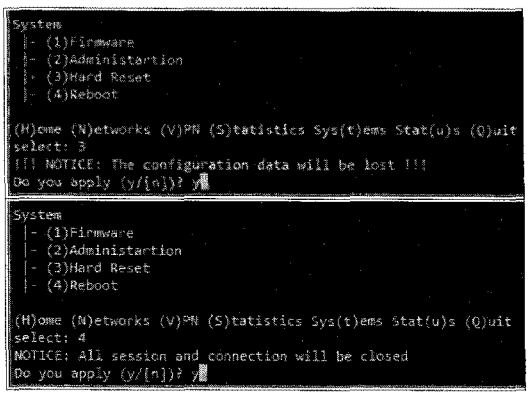
〔그림 9〕 IKE관리(telnet 및 HTTP)

본적으로 상대 노드의 주소와 IPSec이 서비스 중인 포트가 필요하다. 만약 상대 노드가 관리하는 서브넷의 주소가 VPN Gateway LAN 설정과 상이한 경우 상대 사설 네트워크 주소를 입력하여 변경할 수 있다. 터널 설정은 telnet 및 HTTP를 통해 설정 가능하다.

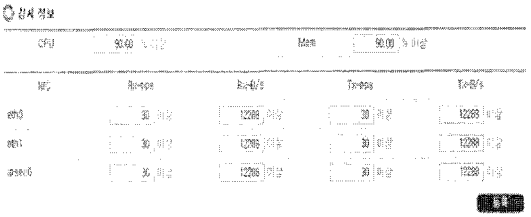
IKE(Internet Key Exchange)는 IPSec 보안 협약을 하기 위한 표준 프로토콜로써 보안상 안전하지 않은 인터넷을 통하여 안전하게 양자 간에 키를 공유하기 위한 프로토콜이다. IKE로 생성된 키는 일정 시간의 수명을 가지며, 이 시간이 만료되면 키를 사용할 수 없기 때문에 만료되기 전 자동적으로 갱신한다. IKE를 통하여 보안 터널이 협약된 경우 SPI(Security Policy Index)가 존재한다. IKE Lifetime은 키의 유효 기한을 의미하며, Re-key margin은 유효기한이 종료되기 전에 IKE 재협상을 하는 여백 기간을 의미한다.

4.2.2 장애 관리

VPN Gateway 장애 발생 시, VPN Gateway를 원상 복구하기 위한 메뉴로, 공장 초기화 및 장비



〔그림 10〕 telnet을 통한 공장초기화 및 장비재부팅



〔그림 11〕 감시 정보 등록(HTTP)

재부팅을 telnet 및 HTTP를 통해 가능하도록 했다. 공장 초기화의 경우 설정 값이 초기화 되는 반면, 장비 재부팅의 경우 기존 설정은 보호되도록 만들었다.

4.2.3 성능 관리

스마트그리드 환경에서 최적화되어 동작하도록 하기 위해서는 VPN Gateway의 성능 관리가 필수적이다. 이를 위해 지속적으로 VPN Gateway의 자원을 감시하고 있는 감시 소프트웨어를 동작하도록 하였다. 감시정보는 VPN Gateway의 자원이 특정 수준 이상으로 할당되어 VPN Gateway가 비정상적으로 동작하는 것을 기 설정된 원격 감시서버에 전달하기 위한 정보이다. 아래 〔그림 11〕의 예는 HTTP를 통한 감시정보 등록 예이다. 이를 통해 앞에서 설정한 trap서버에 해당정보를 push하여 관리하도록 하였다.

4.2.4 감사 관리

감사(Audit)는 Linux syslog의 로그 방식을 이용하여 flash memory에 저장하며 다음과 같은 종류의 정보를 기록한다.

4.2.5 연동 및 공인시험기관 평가

개발된 제품으로 기 상용제품(퓨쳐시스템社)과 연동 테스트를 하여 ARIA 암호화 알고리즘을 이용한

〔표 9〕 감사 정보 종류

분 류	기록 시점
관리자 작업	관리자 로그인, 시스템 설정 변경
서비스 실행 및 종료	서비스 실행, 서비스 종료
VPN 세션 연결/종료	세션 연결/실패, 세션 종료
장비 장애	예기치 못한 장비의 장애 발생

〔표 10〕 연동 및 인증기관 시험 결과

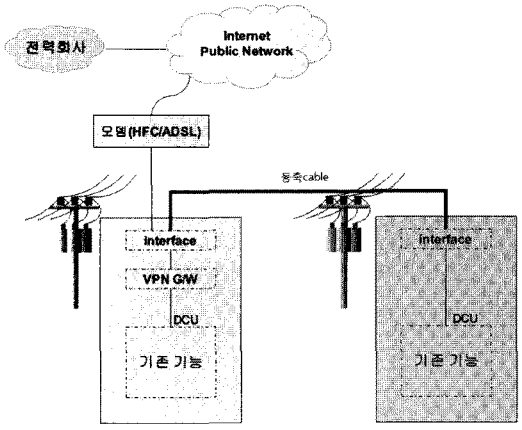
구 분	내 용	결 과
상용제품 연동시험	상용제품(퓨쳐시스템社) 연동(ARIA암호알고리즘)	암호화 처리속도 약 580Kbps
고온 방치 시험	KOLAS 시험 (한국교정시험기관인정기구) KS C 0221(고온시험) 70℃ : 16시간 유지	시험합격(2009-E0288) 육안검사 및 data logging 이상 없음
저온 방치 시험	KOLAS 시험 KS C 0220(저온시험) 25℃ : 16시간 유지	시험합격(2009-E0287) 육안검사 및 data logging 이상 없음
온도 변화 시험	KOLAS 시험 KS C 0225(온도변화시험) 상온 → -20℃(3시간 유지) → 70℃(3시간 유지) 조건, 2사이클	시험합격(2009-E0289) 육안검사, data logging 이상 없음
시범 설치	한국전력공사 PLC 저압 원격검침망에 필드형 VPN Gateway 와 기 운영 중인 상용제품과 터널링 구성 및 원격검침 데이터 암호화 통신 구현	IPSec 방식 터널링, ARIA알고리즘으로 암/복호화하여 원격 검침 데이터의 암호화 통신 (무결성, 기밀성 보장)

데이터 송수신 상태를 확인하고, 〔표 10〕에서와 같이 실외에서도 정상적으로 동작이 가능한지 공인된 시험 기관에서 테스트를 해 본 결과 고온 및 저온에서 안정적으로 동작함을 확인하였다.

V. 결 론

우리나라의 전력 분야 제어시스템은 보안에 우수한 폐쇄형 네트워크로 운영되고 있어 보안 피해의 심각성을 대체로 인지하지 못하고 있다. 그러나 회사 직원의 실수나 부족한 정보보호 지식으로 인한 간접적인 피해가 일어날 수 있으며, 앞으로 스마트그리드 사업이 계속 확대되면 스마트 미터에서부터 발전소에 이르기까지 다양한 형태의 사이버 공격이 이루어질 수 있다.

본 연구에서는 스마트그리드로 가면서 외부의 혹독한 환경과 전국적인 망에서의 안정적 데이터 전송과, 침입 방지를 위해 필요한 스마트그리드 환경에 최적화된 필드형 VPN Gateway를 구현하는 것으로, 현재 다양한 형태로 운영되고 있는 PLC 집중화기, 수요관리 시스템, SCADA RTU 현장 조사를 통해 옥내/외 철구함 안에 필드형 VPN Gateway 설치 가능하도록 기기 개발하기 위해 현장실사를 통해 요구사항을 파악하여 필드형 VPN Gateway 개발규격을 확정하였다.



〔그림 12〕 향후 연구방향

스마트그리드 환경에 최적화된 필드형 VPN Gateway를 위해 기 상용제품과 달리 하드웨어 측면에서 옥외 철구함 내에 설치가 되도록 크기를 최소화하였으며, 실외에서도 동작 가능하도록 온도 -20℃~70℃ 및 습도 90%까지 견디도록 제작하였다. 그리고 효율적 운영을 위해 LED와 포트위치를 동일하게 전면부에 배치하였으며 VPN 관련 동작 여부를 LED를 통해 쉽게 파악할 수 있도록 하였고, 차폐 기능이 우수한 알루미늄 케이스로 외관을 구현하였다. 소프트웨어 측면에서는 기 상용제품에서 부가적으로 지원하는 이중화 기능 및 유해사이트 차단 기능을 축소하고, 전력 IT 환경에 필요한 DHCP 서버 기능 및 IP layer data fragmentation 기능과 지속적으로 필드형 VPN Gateway의 자원을 감시하고 있는 감시 소프트웨어를 동작하도록 하였으며, 공장 자동화 및 자체 리부팅 기능을 추가하였다. 또한 스마트그리드 환경에서의 필드형 VPN Gateway의 수요는 꾸준히 증가할 것으로 예상되므로 위와 같은 기능 축소와 함께 경제적 부담까지 줄였다.

완성된 시제품으로 기 운영되고 있는 상용제품과 다양한 방식으로 연동 테스트를 하여 기능 및 안정성을 확인 후, KEPCO(한국전력공사) PLC 저압 원격검침망에 시범 설치되어 보안이 강화된 데이터 통신을 하고 있다. 도입 후 효과로는 IPSec 방식의 터널링 및 ARIA 암호 알고리즘으로 암호화를 하여 PLC 저압 원격검침 데이터를 주고받게 되었다. 즉, 안전한 통신 채널 확보로, 데이터 위·변조 및 해킹으로부터 안전한 통신망을 얻게 되었다. 또한 필드형 VPN Gateway의 DHCP server 기능으로 인해 부가적으로 IP 추가 부여가 불필요하게 되어 전용회선 비용

절감 효과를 가지게 되었다.

향후, 스마트그리드의 주요 분야 중 하나인 AMI (Advanced Metering Infrastructure)에서 사용이 가능하도록 원격검침 기능을 수행하는 장비 내에 VPN S/W 기능을 넣어서, 단순화 연구를 진행할 예정이다. 즉 기존 DCU 기능에 VPN S/W 기능을 넣어 비용 절감을 하는 것으로, 안정적 데이터 통신을 위해서는 기능 통합이 이루어져야 되겠다.

참고문헌

[1] 이건희, 서정택, 이철원, "스마트그리드와 사이버 보안", 한국통신학회, 정보와통신, 27(4), pp. 23-25, 2010년 4월.

[2] 윤인하, "최근 미국 동부지역의 정전사태와 미국 전력산업의 문제점", 한양대학교 아태지역연구센터, 쟁점과 연구 통권 제140호, pp.23-27, 2003년 9월.

[3] 시병권, "알기 쉬운 스마트그리드 해설", 한국조명전기설비학회, 조명,전기설비학회 눈문지, 23(6), pp,71-78, 2009년 12월.

[4] 문승일, "스마트그리드 개념", 한국통신학회, 정보와 통신: 한국통신학회지 27(4), pp.3-9, 2010년 4월.

[5] Jeanne Meserve CNN Homeland Security Correspondent, "Smart Grid may be vulnerable to hackers", http://articles.cnn.com /2009-03-20/tech/smartgrid.vulnerability_1_smart-grid-power-grid-blackout?_s=PM:TECH, CNN News, Mar. 2009.

[6] 도윤미, 김선진, "스마트그리드 기술동향 : 전력망과 정보통신의 융합기술", 한국전자통신연구원, 전자통신동향분석 24(5), pp.74-86, 2009년 10월.

[7] 유남철, 이주연, 오길환, "스마트그리드 추진 동향 및 구현 방안", 정보통신산업진흥원, 주간기술동향 통권 1426호, pp.26-35, 2009년 12월.

[8] 주성호, 임용훈, 백종목, "AMI기반 에너지 관리시스템", 전력전자학회, 2010년도 하계학술대회 논문집 2010, pp.109-110, 2010.

[9] Kory Hamzeh, Grueep Pall, and William Verthein, "Point-to-Point Tunneling Protocol(PPTP)", Internet Society, RFC 2637, Jul. 1997.

[10] S. Kent, R. Atkinson, "Security Architecture for the internet protocol", Internet Society, RFC 2401, Nov. 1998.

[11] S. Kent, R. Atkinson, "IP Authentication Header(AH)", Internet Society, RFC 2402, Nov. 1998.

[12] S. Kent, R. Atkinson, "IP Encapsulation Security Payload(ESP)", Internet Society, RFC 2406, Nov. 1998.

[13] 한국정보통신기술협회, "정보통신 표준화백서 2008", 한국정보통신기술협회, pp.302-303, 2008.

〈著者紹介〉

박 준 영 (Jun Young Park) 학생회원
2004년 2월: 동아대학교 전기전자컴퓨터공학부 졸업
2004년 6월 ~ 현재: 한국전력공사 ICT기획단 정보보호팀
2010년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 네트워크 보안, 컴퓨터 포렌직

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월 ~ 2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월 ~ 현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직