전력전자상거래(VSEM)를 위한 웹기반 미터링/과금 시스템의 보안성 분석 및 평가에 관한 연구

°강환일, °송영기, °°강환수, °°조진형, °장우석
°명지대학교, 정보공학과 hwan@mju.ac.kr, bysie@paran.com, hideto7@hanmail.net
°°동양전문대학교, 전산정보학부 {인터넷 비즈니스과, 모바일 인터넷과} {hskang, cjh}@dongyang,.ac.kr)

A study on the security analysis and evaluation of the web based metering/billing system for the value storage electricity meter

°Hwan Il Kang, °Young Ki Song, °°Hwan Soo Kang, °°Jin Hyung Jo, °Woo Seok Jang
°Dept. of Information Eng., Myongji Univ. hwan@mju.ac.kr, bysie@paran.com, hideto7@hanmail.net
°°Division of Computing & Information, Dept. of {Internet Business, Mobile Internet}Dongyang Tech. College. {hskang, cjh}@dongyang,.ac.kr

ABSTRACT

본 연구는 제4세대 미터링(Metering) 기술을 이용한 전력전자상거래 즉 VSEM(Value Storage Electricity Meter)을 위한 웹기반 미터링 시스템의 보안성 분석 및 평가에 관한 연구이다. 특히 수요자 측면에서 스마트카드(지불결제)를 이용한 본인확인(SIM카드), 키 값 확인, VSEM서버에서의 각 수요자와 공급자 데이터 사이의 무결성 확인(Integrity)과 부인 방지(Non-repudiation)를 위한 기존 시스템의 보안 문제를 분석하고 이를 해결할 수 있는 보안 모델을 제안한다..

1. 서 론

전력 시스템은 그 자체가 국가적인 인프라이며, 최근 정보기술의 발전에 따라 다양한 모델의 서비스가 전개되고 있다[1]. 특히 통신산업의 경우, 선불 및 후불제와 같은 요금 정산 방식을 통해 산업의 경쟁과 효율을 높이고 있지만 전력 산업은 아직 그 적용이 확대되고 있지 못한 상황이다. 전력 사용에 대한 미터링 기술은 기계식 미터링 기술을 제1세대라고 하며, 원격검침방식을 2세대 그리고 영국에서 개발된 3세대기술은 선불 카드(Prepaid card)에 금액 정보가 입력하여 이 카드를 전력량계에 삽입하여, 그 요금만큼 사용할 수 있도록 하였다. 최근에는 전기는 저장할 수 없는 특성 때문에 생산시점에서 즉시 소비되어야 하며, 전력회사들은 시간대별 수요량에 대한 117%의 예비율 확보를 해야 한다.[2]

이러한 적정한 예비율 확보, 전력 판매의 경쟁체제 도입 및 재판매에 대한 시장 요구에 부합하기 위해 추진되고 있는 전력전자상거래(VSEM;Value Storage Electricity Meter) 시스템을 구현하기 위해서, 본 연구에서는 VSEM의 사용자 정보 확인을 위한 스마트 카드[3], 미터링과 과금(Billing), 가치 정보(Value data, 예, 비용, 사용량등)의 전송과 인터넷을 통한 예약 서비스 시 발생할 수 있는 보안 문제점을 분석하고 이를 해결하기 위한 보안 모델을 제시한다. 웹기반의 전력 관리는 기존의 반복적인 검침업무 및 분석을 자동화하여 보다 효율적으로 전력사용량 및 부하사용량을 파악하고, 이를 자동으로 분석할 수 있도록 디지털 장치와 소프트웨어를 개발한 연구[4]를 진행했지만, 보안 관점에서의 분석 및 평가는 없었다. 본 연구에서는 웹기반의 전력전자상거래 시스템의 적용을 위한 모델을 제시하고 이를 구축하기 위해 필요한 보안 모델을 제시한다. 2장에서는 제안 전력전자상거래 시스템의 구성과 세부 구성요소에 대해 설명하고 3장에서는 보안 취약성 분석 및 제안 보안 모델에 대한 평가를 수행한다. 마지막 장에서는 VSEM의 구축에 대한 향후 연구 방향과 문제점에 대해 제시한다.

2. 전력전자상거래(VSEM) 시스템의 개요

전력전자상거래 기존의 미터링 기술의 단점을 보완하고 전력 공급의 경쟁 체제를 통한 판매를 이루기 위해 개발된 기술로, 그 개략적인 구성은 그림1 같다.

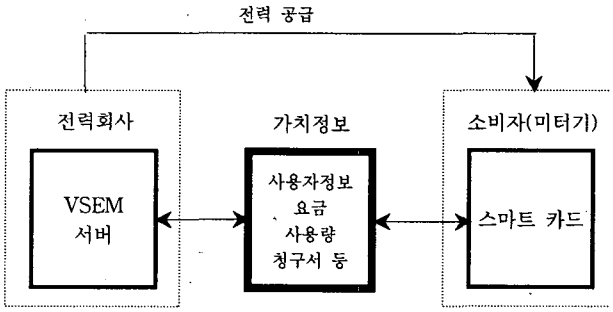

그림 1 VSEM의 개략적 구성도

여기서, VSEM미터기(소비자 측면)내부에는 선불이나 후불로 사용 비용을 정산(Billing)할 수 있는 전자 지갑(electronic wallet) 기능을 가지고 있다. 미터기와 과금 장치에 의해 사용자의 전력 사용에 대한 가치 정보를 생성하고 이를 과금하기 위해 전자 청구서를 작성하여 VSEM서버로 보내지게 되고 이를 통해 전력 공급자는 전력 예비율에 대한 통계적 데이터를 통해 공급의 효율성을 기할 수 있다. VESM의 미터기에는 전력 사용량 정보 계측기, 실시간 요금 계산기, 표시부 및 사용량 디지털 변환 장치를 가지고 있으며, 사용량에 따른 과금을 위해 스마트 카드를 가지고 있다. 이러한 전력 가치 수집 정보는 블루투스(Bluetooth)혹은 RF모듈등 최근의 홈네크웍 내의 전력

선통신등을 이용하여 VSEM서버로 보내 진다. 전력 전자 상거래 시스템은 기존의 전력 공급/수급에서 사용되는 일체의 과금/결제 수단이 갖는 기능을 인터넷 등과 같은 개방형 네트워크를 기반으로 이루어지게 하기 위하여 디지털 정보보호기술(예, 스마트카드보호 기술)과 네트워크 기술을 바탕으로 특히 적용의 용이성과 편리성, 위조 및 이중사용 방지 기능 등에 관한 정보기술(information technology)이 핵심 요소 기술이다.

2.1 스마트 카드의 구조

본 절에서는 전력 전자상거래를 기술을 구현하기 위해 핵심적인 구성요소 중 하나인 스마트카드(Smart Card)에 대해서 기술한다. 스마트 카드는 안전한 보안 매체로써, 신분증, 금융카드(신용카드) 및 교통, 통신등에 널리 사용되고 있다. 스마트 카드는 크게 사용하는 운영체제(COS;Chip Operating System)에 따라 폐쇄형과 공개형(예, 자바카드, 멀토스)으로 나뉘어지고, 통신 방법에 따라 접촉식/비접촉식으로 구분 된다. 스마트 카드의 내부구조를 살펴보면 아래 그림과 같다[5,6].

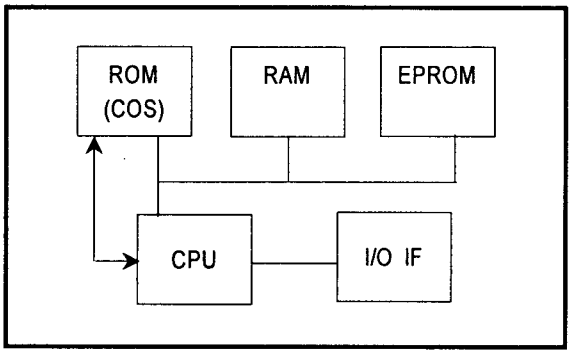

그림 2 스마트 카드의 내부 구성도

2.2 전력 전자 상거래를 위한 주요 보안 이슈 사항

인터넷이란 정보의 공유와 개방을 목표로 개발되었기 때문에 기본적으로 보안에 취약한 개방형 구조로 되어 있다. 따라서 수반하는 보안 문제를 해결하기 위한 기술이 요구되는데 인증, 기밀성, 무결성, 부인방지 등을 만족하여야 한다. 이를 위한 전력 전자상거래의 보안은 주로 암호화 기술은 활용하여 이루어진다. 암호화 기법에는 비밀키 방식, 공개키 방식이 있으며 이러한 암호화 기법을 활용한 암호화 프로토콜을 이용하여 보안에 이용하고 있으며 인증서비스가 상용화 되어 제공되기에 이르렀다. 구매자와 판매자사이의 과금서비스를 제공하기 위한 기술로.다양한 형태의 지불시스템이 개발되고 있다. 대표적인 지불시스템으로는 신용카드를 전자상거래의 지불수단으로 활용하기 위한 신용카드 기반의 지불시스템, 사이버 뱅킹을 이용한 지불시스템, 전자화폐 기반의 지불시스템 등이 있다. 이중 차세대 결제방법으로 주목받고 있는 네트워크형과 IC카드형이 있는데 IC카드형이 주류를 이루고 있으며 대표적으로 몬덱스 등이 있다. 또한 전력 전자상거래를 위한 정보탐색 기술, 차세대 인터페이스 기술, 실시간 B2B, B2C간 거래 기술 등이 필요하며, 현재 국내에는 기반 인프라의 도입이 이루어져 있다. 또한 유럽의 경우와 같이 소비자의 인증을 보다 강화하기 위해 본인 인증을 위한 바이오인식(지문/얼굴)을 이용한 인증 센터도 적용가능하다.

3. 웹기반 미터링/과금 시스템의 보안 요구 사항

전술한 바와 같이 전력 전자 상거래시스템의 구현을 위해서는 선결과제로 보안 문제를 해결해야 한다. 본 절에서는 전력 전자상거래 시스템을 웹(인터넷)기반으로 구현할 경우 발생할 수 있는 보안 문제점과 이를 해결하기 위한 해결책을 제시하고자 한다. 먼저 웹기반 미터링/과금 시스템을 위한 보안 인증 모델을 구조화 한다. 이는 사용자(소비자)인증, 스마트카드 인증 메카니즘과 미터링 장치,가치 정보의 보안 및 과금, 미터링 장치와 서버의 보안으로 구분할 수 있다.

구분	보안 방법	비 고
사용자	비밀번호, 바이오인식 정보	본인 확인
스마트 카드	인증서, 보안 모듈	
미터링 장비	인증 키	
통신 보안	암호화키(대칭, 비대칭)	보안 프로토콜
가치 정보	메시지 암호화, 무결성	
서버 보안	네크웍 보안(SSL, TSL)	VSEM

위와 같은 보안의 주요 핵심 요소에 따라 본 연구에서는 스마트키를 이용하여 사용자의 신원 정보(바이오인식,ID정보)와 고객 정보를 저장하고, 이를 웹기반 미터링 시스템에 적용하는 방법을 제안한다. 이는 미터링 장비와 과금시 사용자의 정보를 확인하는 기술로, 최근 스마트 환경(Smart Environment)에서 적용되고 있다[7,8]. 사용자가 PIN(Personal Identification Number)를 장치를 통해 입력하여 신분을 확인하고 미터링 장비는 할당된 개인키(Private Key)를 통해 서버와 가치 정보의 무결성(Integrity)과 기밀성(Confidentiality)을 확인할 수 있다. 특히 미터링 장치에 내장된 스마트카드가 능동적인 인증 시스템을 구현할 수 있도록 암호화를 직접수행 할 수 있는 기술의 개발을 통해, 미터링 정보, 과금에 대해 정보의 안정성을 더욱 확보할 수 있다. 이를 통해 다음과 같은 보다 이상적인 미터링 및 과금 시스템의 구현이 가능하다.

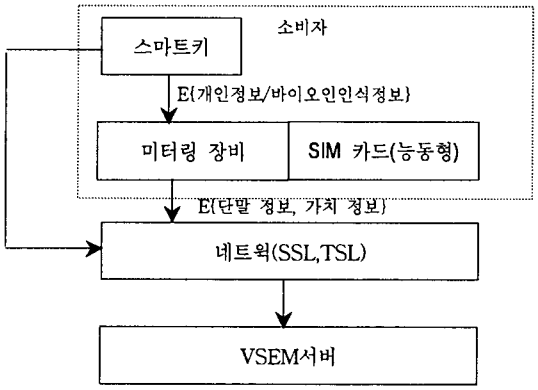

그림 3 제안된 보안 아키텍처

위의 그림에서 보듯이 웹기반 미터링 및 과금 시스템의 구현을 위해서는 소비자 측면에서의 개인정보 및 미터링 정보와 가치 정보의 보안과 단말기에 대한 인증성을 보안을 유지해야 하며, 그 정보는 VSEM서버의 집계시 보안 확인을 통해 보다 안전하게 전력 사용과 과금이 이루어질 수 있다.

4. 결 론

본 연구는 전력 전자 상거래 시스템을 웹기반으로 구현하기 위해 필수적으로 요구되는 보안에 대해 다루고 있다. 특히 웹기반으로 전력 상거래를 하기 위한 선결 조건으로 사용자 보안, 단말기 보안, 가치 정보 보안 및 서버에 대한 보안 아키텍쳐를 제안한다. 특히 능동형 스마트 카드 기술 개발을 통해 사용자 단의 보안이 아닌 단말기 자체의 보안을 더욱 강화할 수 있는 기술 개발을 향후 진행할 예정이다.

이 논문은 기초전력연구소 전력선행연구의 지원(R-2005-7-132-01)으로 수행되었으며 관계 부처에 감사드립니다.

참 고 문 헌

[1] EPRI, Electricity Infrastructure Security Assessment, vol. I-II, EPRI, Palo Alto, CA, Nov. Dec. 2001.

[2] R.J.Anderson, S.J.Bezuidenhout "Cryptographic Credit Control in Pre-payment Metering Systems" p. 15-23,IEEE 1995.

[3] 조대현, "웹기반 전력 관리 시스템", p.37-43, 발전 PLANT 제어계측 기술동향과 적용사례

[4] Andre Dos Santos, "Using Smartcards for Authentication".

[5] Smartcard, http://www.gemplus.com/basics/index.html

[6] 스마트카드 기술 동향.
http://www.kisa.or.kr/technology/sub2/current_smartcard.htm

[7] S.Jang, S.Lee, W.Woo, "Research Activities on Smart Environment", IEEE, Magazine, Vol.28, pp.85-97, Dec.2001.

[8] 오유수, 장세이, 우운택, "스마트 키를 이용한 사용자 인증 및 환경 제어", 광주 과학 기술원.