情報保護學會論文誌
第20卷 第6號, 2010. 12

스마트미터의 취약성/보안요구사항 분석 및 CC v3.1 기반 보호프로파일 개발

정 철 조,† 은 선 기, 최 진 호, 오 수 현, 김 환 구‡
호서대학교 정보보호학과

Protection Profile for Smart Meters: Vulnerability and Security Requirements Analysis*

Chul-Jo Jung,† Sun-Ki Eun, Jin-Ho Choi, Soo-Hyun Oh, HwanKoo Kim‡
Dept. of Information Security, Hoseo University

요 약

최근 정부가 발표한 저탄소 녹색성장 사업의 일환으로 스마트 그리드 기술이 주목을 받고 있으며, 이러한 스마트 그리드가 정착되기 위해서는 가정 또는 전력을 소모하는 모든 장소에 스마트미터의 설치가 필요하다. 그러나 최근 들어 스마트미터의 다양한 보안 취약성이 소개되고 있으며, 아직까지 범용의 보호프로파일이 존재하지 않으므로 스마트미터 제품에 대한 안전성을 보증할 수 없는 실정이다. 따라서 본 논문에서는 스마트미터의 보안 취약성과 공격방법을 분석하여 스마트미터가 일반적으로 갖추어야 할 보안기능과 보안요구사항을 도출하고, 이를 바탕으로 스마트미터 제품의 안전성 평가 및 인증에 사용될 수 있는 공통평가기준 v3.1 기반의 스마트미터 보호프로파일을 개발한다.

ABSTRACT

There is a growing interest in "smart grid" technology, especially after the government recently announced "low-carbon green-growth industry" project. A smart grid uses "smart meters", which can be deployed in any power-consuming places like homes and factories. It has been shown that smart meters have several security weaknesses. There is, however, no protection profile available for smart meters, which means that safety with using them is not guaranteed at all. This paper analyzes vulnerabilities of smart meters and the relevant attack methods, thereby deriving the security functions and requirements for smart meters. Finally, we propose a protection profile based on Common Criterion v3.1 for smart meters.

Keywords: Smart grid, Smart meters, Protection Profile

I. 서 론

최근 들어, 저탄소 녹색성장이 전 지구적 과제로 등장하면서 온실가스 배출을 최소화하는 그린에너지 산업의 핵심으로 스마트 그리드(Smart Grid) 개념이 출현하였다. 스마트 그리드는 기존 전력망에 IT 기술을 접목해 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망 기술이다[1]. 스마트 그리드는 기존 전력망과 비교하여 전력 계통을 규모에 따라 분산적이고 독립적으로 운영할 수 있는 유연성을 지니며, 각 계통에 센서 및 미터들을 장착하여 소비자의 요구에 실시간으로 반응할 수 있는 장점이 있다. 현재 우리 정부는 첨단 검침 인프라(AMI: Advanced Metering Infrastructure) 구

접수일(2010년 8월 31일), 수정일(2010년 11월 12일), 게재확정일(2010년 11월 23일)
† 주저자, jchuljo@nate.com
‡ 교신저자, hkkim@hoseo.edu

축 산업을 적극적으로 진행하고 있으며, 점진적으로 전력을 사용하는 가정 및 모든 장소에 스마트미터(smart meter) 보급을 추진하고 있다[2]. 스마트미터란 시간대별 사용량을 측정하고 그 정보를 송신할 수 있는 기능을 갖춘 전자식 전력량계로써 기존 전력 미터기와 달리 LCD 디스플레이를 이용하여 전력 사용량을 실시간으로 체크하고 전력 공급자와 양방향 통신을 통해 검침비용 및 에너지 절약 등의 효과를 거둘 수 있도록 도움을 주는 기기이다. 그러나 최근 들어 보안전문 업체인 InGuardians와 IOActive 등에 의해 스마트미터 제품들에 대한 취약성 및 공격방법이 소개되고, 스마트미터에서 전송되는 전력사용량에 대한 정보가 개인 프라이버시 문제를 야기할 수 있다는 문제들이 제기되면서 스마트미터의 안전성에 대한 중요성이 부각되고 있다[3,4]. 일반적으로 국내·외에서는 보안성이 포함된 IT 제품의 안전성과 신뢰성을 강화하고 검증된 제품의 공급으로 국가 및 공공의 정보보호 수준을 제고하기 위해 공통평가기준(CC: Common Criteria)을 통해 제품에 대한 안전성 검증 및 평가/보증 제도를 시행하고 있다[5,6]. 하지만, 스마트미터에 대한 범용 보호프로파일의 부재로 이러한 안전성 검증 및 평가가 어려운 실정이며, 따라서 본 논문에서는 스마트미터의 취약성 분석을 통해 보안요구사항을 도출하고, 이를 기반으로 스마트미터 보호프로파일을 개발한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트 그리드와 스마트미터의 취약성 및 공격방법을 소개하고, 3장에서는 스마트미터의 보안성 평가를 위해 TOE(Target of Evaluation)를 정의하며, TOE와 TOE의 환경에 적합한 보안기능 요구사항을 도출한다. 마지막으로 4장에서는 논문의 결론을 맺도록 한다.

II. 관련연구

2.1 스마트 그리드

스마트 그리드는 기존의 중앙 집중형이고 일방향적인 전력 계통의 비효율성을 극복하고 에너지 낭비를 줄이기 위해 기존의 전력망에 정보기술이나 첨단기술을 활용한 차세대 전력망이다. 이러한 스마트 그리드는 전력과 정보의 양방향 흐름을 가짐으로써 분산화된 전력 시스템을 구축할 수 있고 전력 소비자에게 보다 다양한 서비스를 제공할 수 있다. 분산화된 전력 시스템이란 지역적으로 넓은 범위에서 태양광, 풍력, 조력 등과 같은 친환경적인 신재생 에너지를 이용하여 대규모 전력을 일괄적으로 공급하고 관리할 수 있는 시스템으로써 스마트 그리드에서는 통신망을 통해 신재생 에너지의 불규칙적인 전력 생산성을 보다 원활하게 제어할 수 있게 된다.

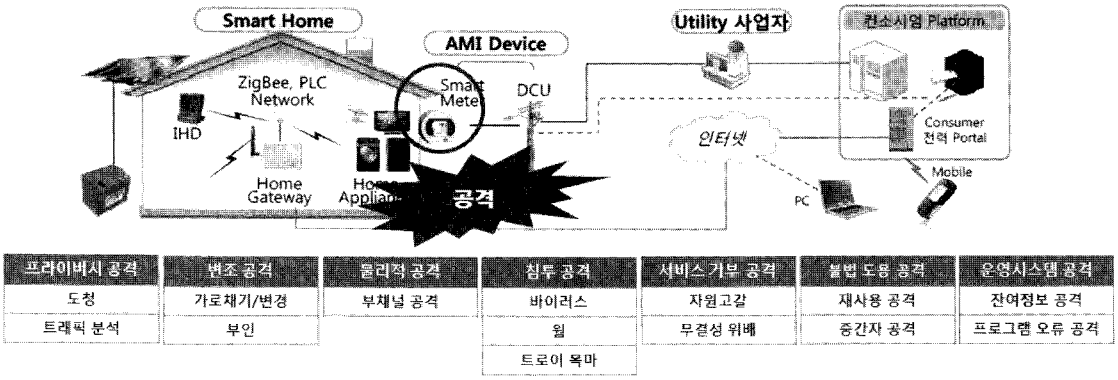
이러한 특징을 지닌 스마트 그리드를 구축하기 위해서는 스마트미터, AMI, 양방향 정보통신 시스템, 감시 모니터링/진단 설비 등의 다양한 장비들이 사용된다. 특히, 이 중 스마트미터는 전력을 사용하는 가정 및 빌딩 등에 설치되어 소비자에게 에너지 소비의 효율성을 제공한다. 스마트미터는 소비자의 전력 사용량을 임의로 정해진 시간 단위로 전력관리서버에 전송하며, 공급자는 이러한 소비자의 전력 사용 정보를 통해 수급 상황별 차등 요금제를 적용하여 전력 수요를 분산시키고 전력 소비자들에게 실시간 전력 사용량을 보여줌으로써 자발적인 에너지 절약을 유도할 수 있다.

2.2 스마트미터에 대한 주요 공격방법

스마트미터에 대한 주요 공격방법은 2009년 InGuardians사에서 발표한 보고서를 기반으로[3], 그림 1과 같이 프라이버시 공격, 변조 공격, 물리적 공격, 침투 공격, 서비스 거부 공격, 불법 도용 공격, 운영시스템 공격으로 분류되며, 이러한 공격들은 심각한 국가적 재난을 야기할 수 있다. 본 절에서는 각 공격들을 예방하기 위한 대응책들을 함께 제시한다.

2.2.1 프라이버시 공격

스마트미터는 일반적으로 15분마다 전력 사용에 대한 정보를 중앙으로 전송한다. 이 때, 총 전력 사용량뿐만 아니라 개별 가전제품에서의 전기 사용량에 대한 정보 등도 같이 전송될 수 있다. 이러한 정보들을 바탕으로 다양한 전력사용 요금체계의 적용과 전기절약 효과를 거둘 수 있는 긍정적인 측면이 존재하는 반면, 정부와 전력회사들에 의해 에너지 소비정보가 악용될 수 있는 문제도 존재한다. 또한 제3자에 의한 프라이버시 침해 문제도 존재하며, 이러한 침해는 도청 및 트래픽 분석과 같은 수동적 공격을 통해 소비자의 전력소비 패턴 또는 특정 전자제품에 관한 사용 여부 등을 파악할 수 있다. 그러므로 프라이버시 침해 공격을 막기 위해서는 송신되는 전력 정보가 평문으로 전송되지 않도록 스마트미터에서 전송하는 정보에 암호화 기술을 적용하여, 제 3자가 도청 및 데이터 수집을 수행하더라도 실제 정보를 얻지 못하도록 하여야 한다.



〔그림 1〕 스마트미터의 공격방법

2.2.2 변조 공격

변조 공격의 목적은 스마트미터에서 전송되는 전력 정보를 중간에서 가로채어 전력 사용량을 변경하는 것으로, 올바른 검침이 되지 않도록 방해하는 공격이다. 이 공격을 통하여 작게는 가정, 크게는 국가 전체의 전력 사용량을 올바르게 확인할 수 없게 되며, 결국 국가적 혼란을 야기할 수 있다. 이러한 변조 공격을 예방하기 위해서는 스마트미터에서 전송되는 정보에 전자서명 기술을 적용하여 인증, 무결성, 부인방지 서비스를 제공할 수 있도록 해야 한다. 전자서명 기술을 스마트미터에 적용하기 위해서는 신뢰된 인증기관이 필요하며, 스마트미터 내 인증서를 저장하는 방식이 도입될 필요성이 있다.

2.2.3 물리적 공격

물리적 공격이란 원격지에 설치되어 있는 스마트미터 내부에 직접적으로 접근하여 스마트미터 내에 적재되어 있는 프로그램 및 데이터 등을 변경하거나 유출하려는 공격을 말한다. 특히 프로빙 공격, 타이밍 공격, 전력 분석 공격과 같은 부채널 공격(Side Channel Attack)을 이용하여 스마트미터 내부의 모듈 칩과 암호 칩에 사용되는 전력에 대한 데이터와 암호화 키, 암호 파라미터 등을 유추할 수 있다. 이를 방지하기 위해서는 스마트미터를 물리적으로 보호된 장소에 위치하도록 하고, 부채널 공격을 방어하기 위한 알고리즘 사용 및 회로에 대한 보호가 필요하다.

2.2.4 침투 공격

침투 공격은 바이러스, 웜, 트로이 목마와 같은 악성코드를 스마트미터에 침투시키는 공격이다. 이 공격은 스마트미터의 원활한 검침활동을 방해하며, 나아가 감염된 정보를 수신하는 전력 공급자의 전산망에도 침투할 수 있는 가능성이 있다. 따라서 이와 같은 악성코드들이 주입되지 않도록, 사용하지 않는 포트(Port)들을 차단하는 것이 중요하며, 안전한 통신을 보장하기 위해 표준 통신 규약을 준수해야 한다.

2.2.5 서비스 거부 공격(DoS: Denial of Service)

서비스 거부 공격의 목적은 스마트미터가 처리할 수 있는 연산능력, 데이터 송·수신능력 그리고 데이터 저장 능력 등을 의도적으로 초과하도록 하여, 제품 자체의 기능을 마비시키는데 있다. 이 공격을 예방하기 위해서는 제품이 일반적으로 처리 및 저장하는 경우의 시그니처를 파악하여, 이에 대한 한계치를 미리 설정하도록 하고, 서비스 거부 공격을 탐지할 수 있는 모듈 및 프로그램을 갖추어야 한다.

2.2.6 불법 도용 공격

이 공격은 중간자 공격(Man-in-the-Middle Attack)과 재사용 공격(Replay Attack)으로 나뉘며, 이러한 공격을 통하여 제3자는 정보를 주고받는 양쪽에서 들키지 않고 전력 정보 및 명령들을 도청 또는 변경할 수 있게 된다. 이러한 공격을 예방하기 위해서는 전자서명과 타임스탬프를 통해 신원과 시간적 절차의 확인

이 필요하며, 정보를 송·수신하는 양단간에 가상사설망(VPN: Virtual Private Network) 기술을 도입하여 제3자의 개입을 예방해야 한다.

2.2.7 운영시스템 공격

운영시스템 공격은 시스템 자체에 내재되어 있는 문제점을 이용하여, 스마트미터의 인증 및 허가권과 명령권을 얻을 수 있는 공격으로써, 가장 위험한 공격 방법이다. 이러한 공격은 운영시스템에서 인증, 명령, 계산 등에 사용되고 남은 잔여정보(레지스터, 메모리, 공유 메모리 및 저장장소 등)를 이용한다. 또한 프로그램의 오류를 이용하여 버퍼 오버플로우(Buffer Overflow)와 포맷 스트링(Format String)공격 등을 통해 권한을 얻을 수 있다. 운영시스템 공격을 예방하기 위해서는 사용 후 메모리 해제 등과 같이 잔여정보를 정리하고, 프로그램에 작성 시, 안전한 함수를 사용하도록 해야 한다.

2.3 스마트미터에 대한 취약성 식별

공격자는 공격을 수행하기 위해 먼저 TOE의 취약성을 식별하며, 취약성을 바탕으로 위협, 가정사항, 조직의보안정책을 도출한다[5]. 스마트미터에 관련된 취약성을 [표 1]과 같이 분류할 수 있다.

III. 스마트미터 보호프로파일

3.1 TOE 개요 및 정의

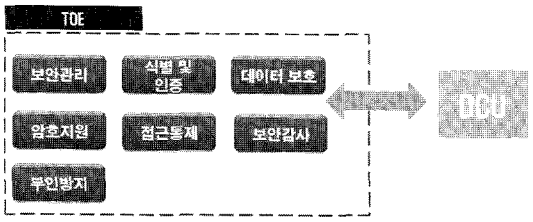
TOE는 무선 통신 기술을 사용한 계량기로써 AMI 통신 구조 내부에 설치하여 운영되며, 기존의 계량기와는 달리 과금 정보 및 사용자의 프라이버시와 관련된 정보들에 대한 불법 도청 및 변조 등의 보안위협이 존재한다. 따라서 TOE를 사용하고자 하는 각 가정 및 빌딩에서는 스마트 그리드 서비스를 안전하게 이용하기 위하여 송수신되는 데이터에 대한 보안관리, 식별 및 인증, 사용자 데이터 보호, 암호지원, 접근통제, 그리고 보안감사, 부인방지 기능 등이 제공되는 스마트미터의 도입이 필요하다.

3.1.1 TOE 범위

일반적인 스마트 그리드 통신 환경에서 스마트미터는 각 가정의 홈 네트워크와 AMI의 게이트웨이 역할을 수행하는 DCU(Data Concentration Unit) 사이에 위치하게 된다. 이러한 스마트미터의 TOE 범위는 [그림 2]와 같이 나타낼 수 있다. 점선으로 나타낸 부분은 스마트미터의 TOE 범위에 해당되며 TOE를 안전하게 관리 및 유지하기 위해 보안관리, 식별 및 인증, 데이터 보호, 암호지원, 접근통제, 보안감사와 부인방지 기능을 제공해야 한다.

[표 1] 스마트미터 관련 취약성 분석

취약성의 종류	설 명
제3의 네트워크를 통한 불법 접근	• 각 계통의 홈 게이트웨이와 연결된 다른 네트워크를 통한 접근
원격 접근 취약성	• 안전하지 않은 통신 프로토콜의 사용 예) Zigbee 통신
평문으로의 전송	• TOE와 외부 IT 실체간의 전송이 암호화 되지 않은 상태로 전송
물리적 공격 취약성	• 안전하지 않은 암호 알고리즘과 보호되지 않은 회로의 사용으로 인한 데이터 및 암호관련 정보 누출
위험 탐지의 부족	• 서비스거부 공격, 바이러스 침입 등의 시도에 관한 사전 탐지 능력 미흡
키 관리 미흡	• 저장된 키와 패스워드 관리 부족, 공개키 구조의 키 분배 문제 미흡
위험 평가의 부족	• 보안, 조직의 보안 위험에 대응하기 위해 필요한 보안 제어에 대한 이해 부족
빈약한 시스템 개발 과정	• 시스템 개발 과정에서의 시스템 구현, 알고리즘 에러, OS 에러로 인하여 시스템 해킹의 단서를 제공
불충분한 시스템 보안	• 약한 패스워드 및 인증 정책, 백업, 복구에 관한 정책 및 시스템 부재



〔그림 2〕 TOE 범위

3.1.2 TOE 기능

TOE의 안전성을 보장하기 위해 제공되어야 하는 보안기능으로는 보안관리, 식별 및 인증, 사용자 데이터 보호, 암호지원, 접근통제, 보안감사 등이 있으며, 요구되는 각각의 보안기능들은 〔표 2〕와 같다.

3.2 TOE 보안문제 정의

TOE 보안문제는 TOE 및 운영환경에 의해 대응되어야 하는 위협, 수행되어야 하는 조직의 보안정책, 지원되어야 하는 가정사항, 이렇게 세 가지로 구분된다. 위협은 위협원에 의해 TOE 및 TOE의 운영환경에 위험을 초래할 수 있는 모든 요소를 의미하며, 위협원은 〔표 3〕과 같이 전문성, 자원, 악의적 동기에 의해 구분된다. 조직의 보안정책은 TOE를 운영하는 조직이 갖추고 있는 내부의 보안정책을 의미하며, 가정사항은 TOE의 보안목적이 성립하기 위한 필요조건이다. 위협은 TOE 보안목적과 대응하며, 가정사항 및 조직의 보안정책은 환경에 대한 보안목적과 대응한다〔5〕.

최근 NIST의 SGIP(The Smart Grid Interoperability Panel)의 CSWG(Cyber Security Working Group)와 UCAIUG의 OpenSG(Open Smart Grid) 및 ASAP (The AMI Security Acceleration Project)에서는 AMI의 안전한 개발을 위하여 여러 보고서들을 발표하고 있다〔7,8,9〕. 이들 보고서는 AMI의 문제점과 취약성을 분석하고 보안요구사항을 항목별로 도출하고 있다. 본 논문에서는 위의 연구그룹들에서 발표한 문서들을 참고하여 아래 〔표 4〕와 같이 TOE에 대한 보안문제 즉, 위협, 조직의 보안정책, 가정사항을 정의하였다.

〔표 3〕 위협원

위협원	전문성	자원	동기
신뢰된 관리자	낮음/높음	충분	악의적이지 않음
부적절한 행동을 하는 관리자	낮음/높음	충분	악의적 임
이전에 신뢰하던 관리자	낮음/높음	보통	악의적 임
합법적인 일반 사용자	낮음/보통	보통	악의적이지 않음
부적절한 행동을 하는 일반 사용자	낮음/보통	보통	악의적 임
인증하지 않은 외부 객체	높음	최소	악의적 임
지진, 홍수, 화재와 같은 환경적 원인의 위협	-	충분	-

〔표 2〕 TOE의 보안기능

보안기능	내 용
보안관리	TOE는 보안기능, 보안속성, TSF(TOE Security Functionality) 데이터, 보안 역할 등과 관련된 사항을 관리한다.
식별 및 인증	스마트 그리드 서비스를 사용하는 사용자 및 관리자를 식별 및 인증한다.
데이터 보호	데이터를 안전하게 저장하기 위해 메모리 내에 보호영역을 두어, 인가된 사용자만이 이 영역에 접근할 수 있다.
암호지원	TOE는 암호연산, 암호키 생성, 분배 및 파기의 암호키 관리를 수행한다.
접근통제	TOE는 인가된 사용자만이 데이터에 접근할 수 있도록, 접근통제 규칙을 제공한다.
보안감사	TOE는 TOE에 접근하는 사용자 및 시간을 기록해야 하며, 보안과 관련된 사건을 저장하도록 한다.
부인방지	사용자 및 관리자는 TOE로부터/에게 데이터의 송신 또는 수신 여부를 부인할 수 없다.

〔표 4〕 보안문제 정의

보안문제		내 용
위 협	T.도청	위협원은 TOE와 DCU간의 통신을 도청하여 사용자 데이터 및 TSF 데이터를 도출할 수 있다.
	T.위변조	위협원은 TOE 내 사용자 데이터 및 TSF 데이터를 변경하거나 복제하여 신원을 위조하거나 변조할 수 있다.
	T.부인	위협원은 사용자 데이터 및 TSF 데이터의 송수신 여부를 부인할 수 있다.
	T.TSF데이터무단변경	위협원은 버퍼 오버플로우, 포맷 스트링 공격 등으로 TOE를 공격하여 TSF 데이터가 무단으로 변경될 수 있다.
	T.정보노출	위협원은 TOE를 정상적으로 사용하는 동안 TOE로부터 누출된 정보를 악용할 수 있다.
	T.바이러스및웜감염	위협원은 네트워크를 통해서 악의적으로 TOE내에 바이러스 및 웜을 감염시킬 수 있다.
	T.서비스거부공격	위협원은 TOE의 서비스 자원을 비정상적으로 초과 사용하여 정상적인 사용자들의 사용을 방해할 수 있다.
	T.재전송공격	위협원은 인가된 사용자의 인증데이터를 재사용하여 TOE에 접근할 수 있다.
	T.잔여정보	TOE가 자원을 재사용할 경우, 객체의 정보를 적절하게 제거하지 못해 위협원이 정보에 불법적으로 접근할 수 있다.
	T.기록실패	저장용량이 소진되어 TOE의 보안관련 사건이 기록되지 않을 수 있다.
	T.기록변경및삭제	위협원은 TOE에 접근하여 보안사건 관련 기록을 변경 또는 삭제할 수 있다.
	T.고장	TOE가 사용 중에, 외부의 공격 등에 의해 고장이 발생하여 사용자에게 정상적인 서비스를 제공하지 못할 수 있다.
	T.전송무결성	위협원은 TOE가 네트워크상에서 전송하는 데이터를 불법적으로 변경할 수 있다.
	T.연속인증시도	위협원은 연속적으로 인증을 시도하여 TOE에 접근할 수 있다.
조직의보안정책	P.감사	TOE와 통신하는 통신상대로/로부터 전송되는 네트워크 트래픽을 TOE 보안정책에서 명시된 대로 기록하며, 보안사건 관련 기록을 기록한다.
	P.암호 알고리즘	TOE는 안전한 또는 조직의 보안 정책에서 정하는 표준 암호알고리즘을 사용하여야 한다.
	P.비밀성	TOE와 통신하는 통신상대로/로부터 전송되는 네트워크 트래픽을 TOE 보안정책에서 명시한 경우 TOE에 의해서 암·복호화 된다.
	P.안전한관리	인가된 관리자/사용자는 안전한 방법으로 TOE를 관리 및 사용해야 한다.
	P.역할	사용자의 역할은 관리자 및 일반 사용자로 구분되며, 역할에 따라 TOE를 관리하거나 운영해야 한다.
가정사항	A.신뢰된관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리기능에 대해 적절히 교육 받았고, 모든 관리자 지침에 따라 정확하게 의무를 수행한다.
	A.신뢰된사용자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리기능에 대해 적절히 교육 받았고, 모든 사용자 지침에 따라 정확하게 의무를 수행한다.
	A.운영환경분리	TOE를 사용하는 기관(가정 또는 사무실)에서 사용되는 다른 스마트 가전제품들을 통하여 TOE에 접근할 가능성이 존재하기 때문에 운영환경을 TOE와 논리적 또는 물리적으로 분리한다.
	A.운영체제보강	불필요한 운영체제 상의 서비스나 수단 등을 모두 제거하는 작업과 운영체제 상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장한다.

3.3 TOE 보안목적

본 논문에서 제안하는 보안목적을 TOE에 대한 보안목적과 운영환경에 대한 보안목적으로 분류하여 다음과 같이 정의한다. TOE에 대한 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확하게 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야 하는 보안목적이다[10]. [표 5]는 TOE 보안문제에서 정의한 내용을 바탕으로 보안목적을 나타낸 것이다.

[표 5] TOE 보안목적

보안목적		설 명
TOE에 대한 보안목적	O1.가용성	TOE는 우발적 또는 외부의 공격에 의해 고장이 발생 시 최소한의 보안기능을 유지하여 정상적인 서비스를 제공해야 한다.
	O2.감사	TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안 관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 관리자가 적절하게 검토할 수 있는 수단을 제공해야 한다. 또한 감사데이터가 포화 상태로 도달하는 경우, 대응기능을 제공해야 한다.
	O3.관리	TOE는 TOE의 인가된 관리자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.
	O4.식별및인증	TOE는 TOE의 정보 흐름 통제를 받는 IT 실체와 TOE에 접근하고자 하는 TOE 관리자를 식별 후 TOE 접근을 허용하기 전에 사용자의 신원을 인증해야 한다.
	O5.바이러스차단	TOE는 네트워크, 이동식 저장매체 등에서 유입되는 바이러스와 TOE에 존재하는 바이러스를 탐지하고 이에 대한 수단을 제공해야 한다.
	O6.역할	TOE는 사용자 역할을 관리자 및 일반 사용자로 구분해야 하며, 역할에 따른 보안 정책 및 보안기능, 접근제어 기능을 제공해야 한다.
	O7.잔여정보제거	TOE는 TSF가 사용하는 작업영역에 사용 종료 시, 사용자 데이터나 TSF 데이터를 남기지 않는 것을 보장해야 한다.
	O8.정보누출대응	TOE는 정상적으로 사용하는 칩이 누출하는 정보가 악용되지 못하도록 대응수단을 마련해야 한다.
	O9.저장데이터보호	TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
	O10.전송데이터보호	TOE는 전송되는 사용자 데이터 또는 TSF 데이터를 인가되지 않은 노출 및 변경으로부터 보호해야 한다.
운영환경에 대한 보안목적	OE1.생명주기 내 보호	TOE의 제조, 발급 각 과정에 대해 물리적, 인적, 절차적 보안 대책이 수립되어 운영되어야 한다.
	OE2.신뢰된관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대해 적절히 교육을 받았고, 모든 관리 지침 및 행동 절차에 따라 정확하게 의무를 수행해야 한다. 또한 자신의 권한을 타인에게 양도하지 않아야 한다.
	OE3.신뢰된사용자	TOE의 인가된 사용자는 악의가 없으며, TOE 관리 기능에 대해 적절히 교육을 받았고, 모든 관리 지침 및 행동 절차에 따라 정확하게 의무를 수행해야 한다.
	OE4.운영체제보강	TOE 및 운영환경의 인가된 관리자는 운영체제의 취약점에 대한 보강작업을 수행하여 TOE와 다른 응용프로그램간의 간섭이 없음을 보장해야 한다.

〔표 6〕 보안문제와 보안목적 간의 대응

	TOE에 대한 보안목적										운영환경에 대한 보안목적			
	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10	OE1	OE2	OE3	OE4
T.도청										O				
T.위변조									O					
T.부인				O										
T.TSF데이터무단변경									O					
T.정보노출								O						
T.바이러스및웜감염					O									
T.서비스거부공격	O													
T.재전송공격										O				
T.잔여정보							O							
T.기록실패		O												
T.기록변경및삭제		O												
T.고장			O											
T.전송무결성										O				
T.연속인증시도		O		O										
P.감사		O												
P.암호알고리즘														
P.비밀성														
P.안전한관리														
P.역할						O								
A.신뢰된관리자														
A.신뢰된사용자														
A.운영환경분리														
A.운영체제보강														

보안목적의 이론적 근거는 명세한 보안목적이 적합한 보안문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증한다. 그러므로 보안목적의 이론적 근거는 각 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해 다루어지며, 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다루며, 〔표 6〕과 같이 대응된다.

3.4 보안요구 사항

3.4.1 보안기능 요구사항

보안요구사항은 보안기능 요구사항과 보증 요구사항으로 나뉜다. 보안기능 요구사항은 보안목적을 충족하기 위한 TOE 및 IT환경의 요구사항으로써, TOE 및 IT 환경은 보안요구사항의 이행을 통해 보안목적을 달성하며, 보안요구사항은 모든 보안목적을 충족해야 한

다. 〔표 7〕은 공통평가기준 2부로부터 관련 기능 컴포넌트를 선정하여 보안기능 요구사항을 도출한 내용이며, 〔표 9〕는 〔표 7〕에서 도출한 보안기능 요구사항들이 TOE의 보안목적을 달성하는지에 대한 이론적 근거를 제시한 내용이다.

3.4.2 보증 요구사항

보증 요구사항은 TOE가 제공하는 보안기능에 대하여 보증을 하기위한 요구사항을 제시한다. 이러한 보증 요구사항은 공통평가기준 3부의 컴포넌트에 의해 표현되며, 본 논문에서는 윤신숙 등[11]이 제안한 보증등급 산정기준에 의하여 보호프로파일의 평가보증등급은 EAL5로 선정한다. 위협등급 산출은 수치화 접근법과 카테고리 접근법 모두 적용하였으며, 수치화 접근법에 따른 평균값은 11.2를 나타냈고 카테고리 접근법으로 분석한 경우, C4가 전체 항목 중에서 10%이상을 차지하였다. 그러므로 위협등급은 T5가 되고 정보가치 V4와 대응되어 EAL5 등급이 된다. 〔표 8〕은 위협등급 산출과정을 나타낸 것이다.

〔표 8〕 위협등급 산출

	수치화 접근법				
	공격 자원	공격 기술	결과 강도	위험 경감 순위	발생 가능성
T.도청	1	1	2	2	1
T.위변조	2	1	3	2	1
T.부인	1	1	1	2	1
T.TSF데이터무단변경	2	3	3	1	3
T.정보노출	3	3	2	1	3
T.바이러스및웜감염	2	3	3	2	2
T.서비스 거부 공격	3	2	3	1	1
T.재전송 공격	1	1	2	2	1
T. 잔여정보	1	1	2	2	1
T.기록실패	1	1	1	2	1
T.기록변경 및 삭제	1	1	1	2	1
T.고장	1	1	1	2	2
T.전송무결성	1	1	2	2	2
T.연속인증시도	1	1	2	2	1
결과	(42+42+28+25+20)/14=11.2				
카테고리 접근법	C2=3, C3=8, C4=3(개) C4=21%				

〔표 7〕 보안기능 요구사항

보안기능 클래스	보안기능 컴포넌트	
보안 감사	FAU_ARP.1	보안 경보
	FAU_GEN.1	감사 데이터 생성
	FAU_SAA.1	잠재적인 위반분석
	FAU_SAA.2	프로파일에 기반한 비정상 행위 탐지
	FAU_SAA.3	단순 공격 학습
	FAU_SAR.1	감사 검토
	FAU_SAR.2	감사 검토 권한 제한
	FAU_SAR.3	선택 가능한 감사 검토
	FAU_STG.1	감사 증적 보호
	FAU_STG.2	감사 데이터의 가용성 보장
	FAU_STG.3	감사 데이터 손실예측 시 대응행동
	FAU_STG.4	감사 데이터의 손실방지
암호 지원	FCS_CKM.1	암호키 생성
	FCS_CKM.2	암호키 분배
	FCS_CKM.3	암호키 접근
	FCS_CKM.4	암호키 파기
	FCS_COP.1	암호연산

보안기능 클래스	보안기능 컴포넌트	
사용자 데이터 보호	FDP_ACC.1	부분적인 접근통제
	FDP_ACF.1	보안속성에 기반한 접근통제
	FDP_DAU.1	기본적인 데이터 인증
	FDP_ETC.2	보안속성을 포함한 사용자 데이터 유출
	FDP_RIP.1	부분적인 잔여정보보호
	FDP_ROL	기본복구
	FDP_SDI.1	저장된 데이터의 무결성 검사
	FDP_UCT.1	기본적인 전송 데이터 비밀성
	FDP_UIT.1	전송 데이터 무결성
식별 및 인증	FIA_AFL.1	인증 실패 처리
	FIA_ATD.1	사용자 속성 정의
	FIA_UAU.1	인증
	FIA_UAU.3	위조할 수 없는 인증
	FIA_UAU.5	재사용 방지 인증 메커니즘
	FIA_UID.1	식별
	FIA_USB.1	사용자-주체 연결
보안 관리	FMT_MOF.1	보안기능 관리
	FMT_MSA.1	보안속성 관리
	FMT_MSA.2	안전한 보안속성
	FMT_MSA.3	정적 속성 관리
	FMT_MTD.1	TSF 데이터 관리
	FMT_SMF.1	관리기능 명세
	FMT_SMR.1	보안 역할
자원 활용	FRU_FLT.1	오류에 대한 내성: 부분적용
	FRU_PRS.1	자원사용 우선순위: 부분적용
TSF 간 안전한 채널	FTP_ITC.1	TSF간 안전한 채널
TSF 보호	FPT_FLS.1	장애 시 안전한 상태 유지
	FPT_ITA.1	외부전송 TSF 데이터의 가용성
	FTP_ITC.1	외부전송 TSF 데이터의 비밀성
	FTP_RPL.1	재사용 공격 탐지 및 대응행동
	FPT_STM.1	신뢰할 수 있는 타임스탬프
	FPT_TST.1	TSF 자체 시험
통신	FCO_NRO.2	강제적인 발신 증명
	FCO_NRR.2	강제적인 수신 증명
바이러스 차단 (확장)	FAV_ART.1	바이러스 경고
	FAV_DTN.1	바이러스 탐지
	FAV_RES.1	바이러스 대응

〔표 9〕 보안문제와 보안기능 요구사항 간의 대응

	TOE 보안목적									
	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
FAU_ARP.1		O								
FAU_GEN.1		O								
FAU_SAA.1		O								
FAU_SAA.2		O								
FAU_SAA.3		O								
FAU_SAR.1		O								
FAU_SAR.2		O								
FAU_SAR.3		O								
FAU_STG.1		O								
FAU_STG.2	O	O								
FAU_STG.3		O								
FAU_STG.4		O								
FCS_CKM.1										O
FCS_CKM.2										O
FCS_CKM.3								O		O
FCS_CKM.4										O
FCS_COP.1								O		O
FDP_ACC.1						O				
FDP_ACF.1						O				
FDP_DAU.1				O						
FDP_ETC.2									O	O
FDP_RIP.1							O			
FDP_ROL.1			O							
FDP_SDI.1									O	
FDP_UCT.1										O
FDP_UIT.1										O
FIA_AFL.1				O						
FIA_ATD.1				O		O				
FIA_UAU.1				O						
FIA_UAU.3				O						
FIA_UAU.5				O						
FIA_UID.1				O						
FIA_USB.1				O		O				

〔표 9〕 보안문제와 보안기능 요구사항 간의 대응(계속)

	TOE 보안목적									
	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
FMT_MOF.1			O							
FMT_MSA.1						O				
FMT_MSA.2						O				
FMT_MSA.3						O				
FMT_MTD.1									O	O
FMT_SMF.1			O							
FMT_SMR.1						O				
FRU_FLT.1			O							
FRU_PRS.1			O							
FTP_ITC.1										O
FPT_AMT.1			O							
FPT_FLS.1			O							
FPT_ITA.1	O									
FTP_ITC.1										O
FTP_RPL.1			O							
FPT_STM.1		O	O							
FPT_TST.1			O							
FCO_NRO.2				O						
FCO_NRR.2				O						
FAV_ART.1(확장)					O					
FAV_DTN.1(확장)					O					
FAV_RES.1(확장)					O					

〔표 10〕 보안기능과 보안기능 요구사항 간의 대응

	TOE 보안기능						
	보안 관리	식별 및 인증	데이터 보호	암호 지원	접근 통제	보안 감사	부인 방지
FAU_ARP.1						O	
FAU_GEN.1						O	
FAU_SAA.1						O	
FAU_SAA.2						O	
FAU_SAA.3						O	
FAU_SAR.1						O	
FAU_SAR.2						O	
FAU_SAR.3						O	

〔표 10〕 보안기능과 보안기능 요구사항 간의 대응(계속)

	TOE 보안기능						
	보안 관리	식별 및 인증	데이터 보호	암호 지원	접근 통제	보안 감사	부인 방지
FAU_STG.1						O	
FAU_STG.2						O	
FAU_STG.3						O	
FAU_STG.4						O	
FCS_CKM.1				O			
FCS_CKM.2				O			
FCS_CKM.3				O			
FCS_CKM.4				O			
FCS_COP.1				O			
FDP_ACC.1					O		
FDP_ACF.1					O		
FDP_DAU.1		O	O				
FDP_ETC.2			O		O		
FDP_RIP.1			O				
FDP_ROL			O				
FDP_SDI.1			O				
FDP_UCT.1			O				
FDP_UIT.1			O				
FIA_AFL.1		O					
FIA_ATD.1		O					
FIA_UAU.1		O					
FIA_UAU.3		O					
FIA_UAU.5		O					
FIA_UID.1		O					
FIA_USB.1		O			O		
FMT_MOF.1	O						
FMT_MSA.1	O						
FMT_MSA.2	O						
FMT_MSA.3	O						
FMT_MTD.1	O						
FMT_SMF.1	O						

〔표 10〕 보안기능과 보안기능 요구사항 간의 대응(계속)

	TOE 보안기능						
	보안 관리	식별 및 인증	데이터 보호	암호 지원	접근 통제	보안 감사	부인 방지
FMT_SMR.1	O				O		
FRU_FLT.1	O						
FRU_PRS.1	O						
FTP_ITC.1			O				
FPT_AMT.1	O						
FPT_FLS.1	O						
FPT_ITA.1			O				
FTP_ITC.1			O				
FTP_RPL.1			O				
FPT_STM.1	O						
FPT_TST.1	O						
FCO_NRO.2							O
FCO_NRR.2							O
FAV_ART.1(확장)			O				
FAV_DTN.1(확장)			O				
FAV_RES.1(확장)			O				

IV. 결론

본 논문은 스마트미터의 범용 프로파일이 존재하지 않는 현실에서 스마트미터의 TOE를 정의하고, 보안문제를 분석한 후, 이에 적합한 보안목적을 도출하였다. 도출된 보안목적을 바탕으로 스마트미터에 대한 보안기능 요구사항을 최종적으로 제안하였으며, 제안한 보안기능 요구사항이 보안목적을 만족함을 이론적 근거를 통해 나타내었다. 그러므로 본 논문에서 제안한 스마트미터 보호프로파일을 이용하여 개발자는 명시된 내용들을 준수하여 보호명세서를 작성할 수 있으며, 소비자들은 최소한의 보안기능들을 참조할 수 있다. 또한 본 논문은 스마트미터의 평가 시 참고 자료로 충분히 활용될 수 있을 것이다.

참고문헌

〔1〕 이경복, 독고지은, 유지연, 이숙연, 임종인, "스마트 그리드에서의 소비자 참여와 보안 이슈,"한국정보보호학회지, 19(4), pp. 21-35, 2009년 8월.

〔2〕 지식경제부, "지능형 전력망 추진정책 및 로드맵 수립 계획," 2009. 6.

〔3〕 InGuardians, "Advanved Metering Infrastructure Attack Methodology," 2009.

〔4〕 IOActive, "Securing the Smart Grid," 2010.

〔5〕 Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB, Setp. 2006.

〔6〕 Common Methodology for Information Technology Security Evaluation, Version 3.1, CCMB, Setp. 2006.

〔7〕 NIST-SGIP:CSWG, "Introduction To NISTIR 7628 Guidelines for Smart Grid Cyber Security," 2010.

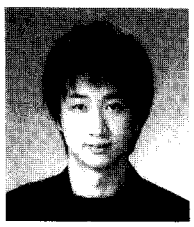
〔8〕 UCAIUG:AMI-SEC-ASAP, "AMI System Security Requirements," 2008.

〔9〕 UCAIUG:ASAP-Smart Grid, "Security Profile for Advanced Metering infras-

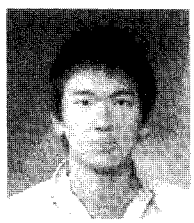
tructure," 2009.
[10] 곽진, 홍순원, 이완석, "보안토큰의 취약성/보안요구사항 분석 및 CC v3.1기반 보호프로파일 개발," 정보보호학회논문지, 18(2), pp. 139-149, 2008년 4월.
[11] 윤신숙, 장대석, 김환구, 오수현, 하재철, 김석우, "보호프로파일 개발을 위한 보증등급 산정 기준에 관한 연구," 정보보호학회지, 17(6), pp. 57-66, 2007년 12월.

〈著者紹介〉

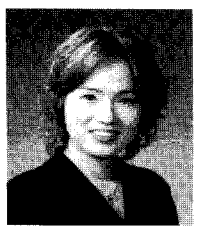
정 철 조 (Chul-Jo Jung) 학생회원
2009년 2월: 호서대학교 정보보호학과 졸업(공학사)
2009년 3월 ~ 현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 보안성 평가, 암호학, 인증



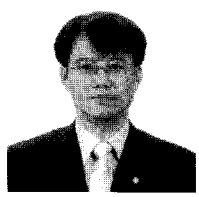
은 선 기 (Sun-Ki Eun) 학생회원
2008년 8월: 호서대학교 정보보호학과 졸업(공학사)
2009년 3월 ~ 현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 네트워크 보안, 스마트그리드 보안, 시스템 평가 및 인증



최 진 호 (Jin-Ho Choi) 학생회원
2010년 2월: 호서대학교 정보보호학과 졸업(공학사)
2010년 3월 ~ 현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 클라우드 컴퓨팅, 네트워크 보안



오 수 현 (Soo-Hyun Oh) 종신회원
1998년 2월: 성균관대학교 정보공학과 졸업(공학사)
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월 ~ 현재: 호서대학교 정보보호학과 조교수
〈관심분야〉 암호학, 네트워크 보안 프로토콜



김 환 구 (HwanKoo Kim) 종신회원
1987년 2월: 경북대학교 수학과 졸업(이학사)
1991년 2월: 경북대학교 대학원 수학과 석사(이학석사)
1998년 2월: U. of Tennessee-Knoxvilie. 수학과. Ph. D.
2002년 3월 ~ 현재: 호서대학교 정보보호학과 부교수
〈관심분야〉 평가 및 인증, 암호학