스마트 홈을 위한 스마트그리드 보호 방안 연구1)

김미주*, 정현철*, 이재일*
*한국인터넷진흥원
e-mail:mijoo.kim, hcjung, jilee@kisa.or.kr

A Study on Smart Grid Security in Smart Home

Mijoo Kim*, Hyun-Cheol Jeong*, Jae-Il Lee*
*Korea Internet & Security Agency

요 약

스마트 홈은 유무선 통신 인프라를 기반으로 댁내 다양한 기기 간 통신을 가능하게 함으로써 사용자에게 원격 에너지 관리, 방범, 의료 등 자동화된 지능형 서비스를 제공할 것으로 기대되고 있다. 이는 기존 전력망에 IT 기술을 융합하여 효율적인 전력 에너지의 송・배전 및 실시간 정보 서비스를 제공하는 스마트 그리드 기술을 기반으로 하고 있으며, 사용자 실생활과 밀접한 관계를 가지기 때문에 보안 문제 발생 시 치명적인 피해를 입힐 수 있다는 특징을 가진다. 이에 본 논문에서는 스마트 홈 및 스마트그리드에 대한 분석을 통해 안전한 스마트 홈을 위한 스마트그리드 보호 방안을 도출한다.

1. 서론

스마트 홈은 유무선 통신 인프라를 기반으로 댁내 다양한 기기 간 통신을 가능하게 함으로써 사용자에게 원격 에너지 관리, 방범, 의료 등 자동화된 지능형 서비스를 제공할 것으로 기대되고 있는 분야이다. 이는 기존의 가전기기를 정보가전기기화 시킴으로서 다양한 서비스 및 부가가치를 창출할 것으로 예상되고 있다.

또한 스마트 홈을 구성함에 있어 주요 기반 기술로 스마트그리드 기술을 들 수 있는데, 이는 기존 전력망에 IT 기술을 융합함으로써 전력 에너지의 효율적인 송・배전 및 실시간 정보 서비스를 제공한다는 특징을 갖는다.

하지만 이 같은 시스템은 사용자 실생활과 직접적인 관계를 가지기 때문에 보안 문제 발생 시 전력공급의 중단, 프라이버시 침해, 과금 오류 등 치명적인 피해를 입힐 수 있다는 점에서 매우 주의 깊게 다뤄져야 한다.

이에 본 논문에서는 스마트 홈 및 스마트그리드에 대한 분석을 통해 안전한 스마트 홈을 위한 스마트그리드 보호 방안을 도출한다.

2. 스마트 홈을 위한 스마트그리드

스마트 홈은 가정 내 정보가전간의 유무선 통신으로 자동화된 전력, 방범, 의료 등의 지능화된 서비스를 누릴 수 있도록 하는 기술로 구성된 주거공간을 말하며, 대표적인 스마트 홈 기술로 모든 디지털 가전기기를 원격 제어할 수 있는 스마트 디지털가전 AV기술, 냉난방 습도 공기 자동관리 등을 하는 에너지관리기술, 가족구성원에 대한 바이오정보를 측정하는 헬스케어기술 등이 있다.

스마트그리드는 기존의 전력망에 IT 기술이 접목되어 전력 공급자와 소비자가 실시간을 전력 사용에 대한 정보를 교환함으로써 에너지 효율성 및 사용자 편의성을 높일 수 있는 기술이다.

(그림 1)은 스마트 홈을 구축하기 위한 스마트그리드의 구성요소를 나타낸다.

스마트 홈을 위한 스마트그리드 구성요소는 구간에 따라 크게 4가지 유형으로 나눌 수 있으며 각각에 해당하는 세부 구성요소는 다음과 같다.

- Service Providers

  요금부과, 집선기, 제3자(공익사업 이외에 중요 기능을 제공하는 업체)

- Operations

  계량기데이터관리시스템, AMI중계소, 고객정보시스템, 정전관리시스템, 부하관리시스템/수요대응관리시스템

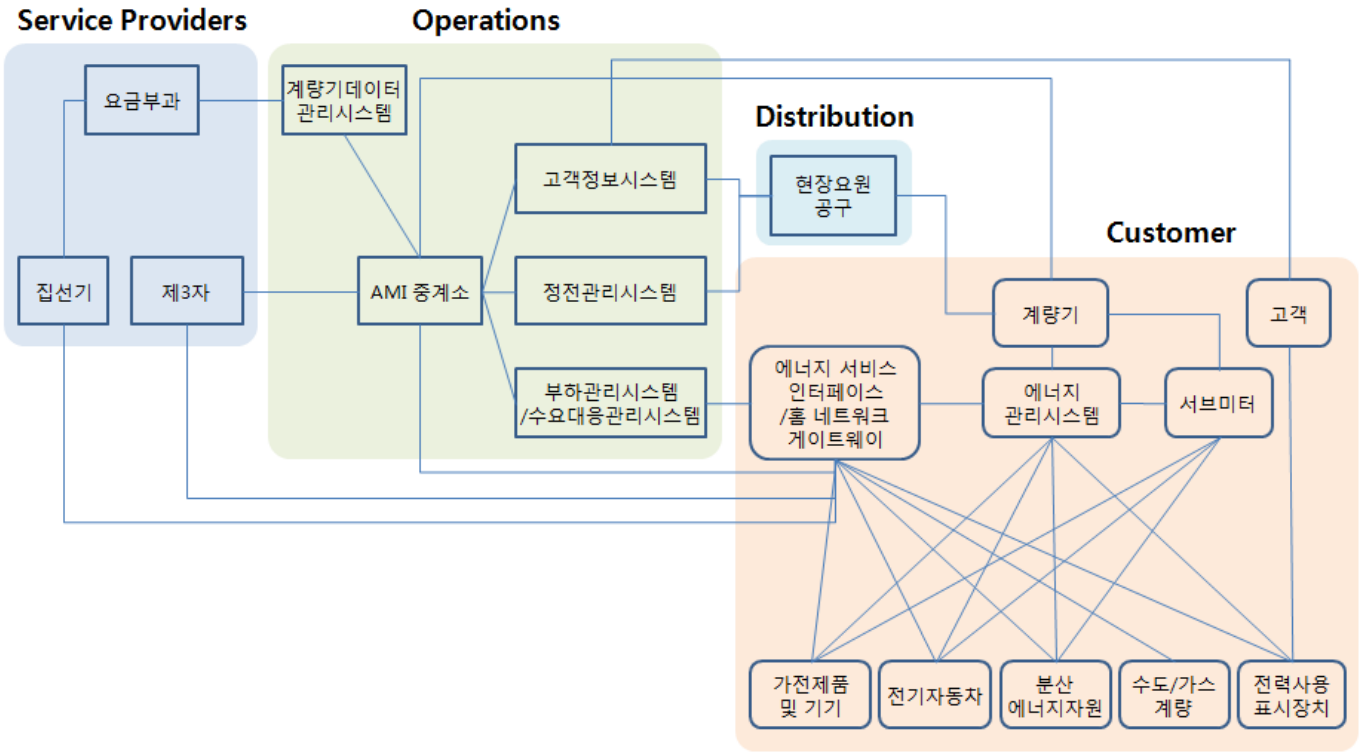
- Distribution

  현장요원공구

- Customer

  고객, 에너지 서비스 인터페이스/홈 네트워크 게이트웨이, 계량기, 에너지관리시스템, 서브미터, 가전제품 및

1) 본 연구는 지식경제부의 지원을 받는 정보통신표준기술력향상사업의 연구결과로 수행되었음



(그림 1) 스마트 홈을 위한 스마트그리드 구성요소

기기, 전기자동차, 분산에너지자원, 수도/가스 계량, 전략사용표시장치

3. 보안 위협

스마트 홈 구축의 기반 기술인 스마트그리드에서 보안 위협은 홈 네트워크 영역이나 LAN 혹은 WAN과 같은 전송망 영역에서도 발생할 수 있으며, 댁내 전력사용량 측정 단말인 스마트 미터에 대한 공격을 통해서도 발생할 수 있다. 또한 관리적인 실수 및 부주의를 통해서도 위험에 노출될 수 있다.

각각에 대한 세부적인 보안 위협은 아래와 같다.

- 홈 네트워크 영역

  홈 네트워크 영역에서 발생할 수 있는 보안 위협으로는 인가되지 않은 장치를 홈 게이트웨이에 연결 및 댁내 장치와의 통신을 시도함으로써 네트워크에 혼란을 가하거나 홈 네트워크 관련 정보를 유출 및 위변조하는 보안 위협이 있을 수 있다. 또한 홈 네트워크 관련 정보에 대한 유출은 가정 사용자의 전력 패턴 등을 노출시킴으로써 프라이버시 침해의 소지가 있다.

- 스마트 미터

  스마트미터는 댁내 전력사용량을 측정하여 그 정보를 전력공급자에 송신하여 사용자가 실시간으로 전력사용량 및 전력사용 비용 등을 확인할 수 있는 장치이다.

  이 과정에서 공격자는 스마트미터의 가격 정보 및 전력 사용량 측정 정보를 위변조하거나 외부로 유출함으로써 소비자에 피해를 유발할 수 있다. 또한, 스마트미터의 특성상 물리적으로 안전하지 않을 수 있는 위치에 설치될 수 있기 때문에 물리적인 공격으로부터 취약할 수밖에 없다.

- 전송(LAN, WAN) 영역

  스마트그리드에서 고객 정보 및 전력량 전송 등에는 LAN이나 WAN 같은 통신 인프라가 활용된다.

  따라서 기존에 통신망의 보안 위협을 상속받아 서비스 방해, 도청, 메시지 위변조, 서비스 거부 공격 등이 보안 위협이 있을 수 있다.

- 관리

  이 영역은 사용자에게 전력서비스를 제공하고 관리하는 공급자 영역이다.

  이 영역에서 발생할 수 있는 보안 위협은 원격 관리로 인한 인가되지 않은 조작, 부주의한 시스템 관리로 인한 악성코드 유입, 내부자의 무분별한 고객 정보 접근 등이 있을 수 있다.

4. 스마트 홈을 위한 스마트그리드 보안 방안

본 절에서는 안전한 스마트 홈 구축을 위한 스마트그리드 보안 방안에 대해서 기술한다. 안전한 스마트 홈 구축

을 위해서는 우선적으로 크게 기밀성, 무결성, 가용성의 요구사항이 충족되어야 한다.

첫 째, 스마트 홈에서는 개인 프라이버시와 재산적 정보를 보호하기 위한 수단을 포함한 정보 접근 및 공개에 관하여 인가된 제한의 유지를 위해서 기밀성이 보장되어야 한다.

둘 째, 스마트 홈에서는 부적절한 정보 변경 또는 폐기의 예방, 그리고 정보 거절 금지 및 인증 등 무결성이 보장되어야 한다.

마지막으로, 스마트 홈은 정보에 대해 시기적절하고 신뢰할 수 있는 접근 및 사용을 가능하게 하는 가용성이 보장되어야 한다.

이러한 세 가지 원칙에 입각하여 안전한 스마트 홈을 구축하기 위해서는 스마트그리드 요소들 간에 다음의 보안 기능들이 요구된다.

- 요금부과-계량기데이터관리시스템

  서비스거부공격 방지, 통신 무결성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 스팸 방지, 권한 관리, 사용자 식별 및 인증, 인가, 장치 식별 및 인증, 패스워드 안전성, 세션 잠금, 감사, 부인 방지

- 요금부과-집선기

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 키관리, PKI인증서, 소프트웨어 무결성, 정보 무결성, 권한 관리, 사용자 식별 및 인증, 패스워드 안전성, 감사

- 집선기-에너지 서비스 인터페이스/홈 네트워크 게이트웨이

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 권한 관리, 사용자 식별 및 인증, 패스워드 안전성, 무선 접속 제한, 감사, 부인 방지

- 제3자-에너지 서비스 인터페이스/홈 네트워크 게이트웨이, 고객정보시스템-고객

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 권한 관리, 사용자 식별 및 인증, 패스워드 안전성, 무선 접속 제한, 감사, 부인 방지

- AMI중계소-계량기데이터관리시스템, 고객정보시스템, 정전관리시스템, 부하관리시스템/수요대응관리시스템

  서비스거부공격 방지, 통신 무결성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 스팸 방지, 권한 관리, 사용자 식별 및 인증, 장치 식별 및 인증, 패스워드 안전성, 세션 잠금, 감사

- AMI중계소-제3자, 에너지 서비스 인터페이스/홈 네트워크 게이트웨이, 부하관리시스템/수요대응관리시스템-에너지 서비스 인터페이스/홈 네트워크 게이트웨이

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 권한 관리, 사용자 식별 및 인증, 패스워드 안전성, 무선 접속 제한, 감사, 부인 방지

- 계량기-AMI 중계소, 에너지관리시스템, 서브미터, 에너지관리시스템-서브미터
- 에너지 서비스 인터페이스/홈 네트워크 게이트웨이-분산에너지자원, 수도/가스 계량
- 서브미터-가전제품 및 기기, 전기자동차, 분산에너지자원

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 사용자 식별 및 인증, 패스워드 안전성, 무선 접속 제한, 감사, 부인 방지

- 현장요원공구-고객정보시스템, 정전관리시스템, 계량기

  메시지 인증, 소프트웨어 무결성, 정보 무결성, 스팸 방지, 권한 관리, 사용자 식별 및 인증, 장치 식별 및 인증, 패스워드 안전성, 세션 잠금, 원격 세션 종료, 휴대용 및 이동장비의 접근 통제, 무선 접속 제한, 감사

- 에너지 서비스 인터페이스/홈 네트워크 게이트웨이-에너지관리시스템

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성, 정보 무결성, 권한 관리, 사용자 식별 및 인증, 패스워드 안전성, 무선 접속 제한, 감사, 부인 방지

- 에너지 서비스 인터페이스/홈 네트워크 게이트웨이-가전제품 및 기기, 전기자동차, 전력사용표시장치
- 에너지관리시스템-가전제품 및 기기, 전기자동차, 분산에너지자원, 전력사용표시장치
- 고객-전력사용표시장치

  서비스거부공격 방지, 통신 무결성, 통신 기밀성, 암호, 키관리, 메시지 인증, 정보 기밀성, 소프트웨어 무결성,

정보 무결성, 권한 관리, 사용자 식별 및 인증, 패스워드 안전성, 무선 접속 제한, 감사, 부인 방지

5. 결론

본 논문에서는 스마트그리드 기술 기반의 스마트 홈 구조 및 보안 위협을 분석하고, 안전한 스마트 홈 구축을 위한 스마트그리드 구성요소 간의 보안 방안에 대해서 알아보았다. 이는 추후 스마트 홈 구축 시 보안 기술 도입에 참고자료로 활용될 수 있을 것으로 기대된다.

참고문헌

[1] NIST DRAFT NISTIR 7628 "Smart Grid Cyber Security Strategy and Requirements", February 2010

[2] Cisco Smart Grid Security Solutions Brief

[3] Pike Research, "Smart Grid Cyber Security: Risk Management, Equipment Protection, Monitoring and Incidence Response, Policy/Planning, and Access/Audit", 1Q 2010

[4] Hanns-Christian L. Hanebeck, "Securing the Smart Grid at the Edge", Smart Grid Cyber Security Summit 1st, August 10 2010

[5] 스마트 그리드 기술 워크샵 2010(SGT 2010), 한국통신학회