AMI 시스템을 위한 보안 기능 설계

양일권*, 최승환*, 김영준*
*한전 전력연구원
e-mail : yangilk@kepco.co.kr

Design of security Method for AMI system

Il-Kwon Yang*, Seung-hwan Choi*, Young-Jun Kim*
*KEPCO Research Institute

요 약

Abstract - 스마트 그리스 환경이 구축되어 고객과 전력회사 간 양방향 서비스가 가능하게 되면 전력회사는 고객에게 IHD 나 ESP 를 통해 여러 전력 서비스를 제공할 수 있게 된다. 더불어 다양한 third party 서비스 업체들도 고객의 정보를 이용한 부가 가치 사업을 개발하여 서비스하게 될 텐데 이 경우 AMI 망을 통한 안전한 정보 공유를 위해 전력망에 대한 보안 정책이 필요하게 된다. 본 논문에서는 국내 실정에 맞는 AMI 기술 개발 및 안전한 운영을 위해 AMI 보안에 관하여 기본적인 요구사항을 분석하고 보안 기능을 설계한다.

1. 서론

본 논문에서는 국내 실정에 맞는 AMI 기술의 안정적 운영을 위하여 AMI 보안을 위한 기본적인 요구사항을 분석 및 열거하고 이를 만족시키기 위한 한국형 AMI (K-AMI)의 보안 구조 설계를 소개하도록 한다.

2. AMI 요구사항

정부에서는 중요 인프라 보호와 산업 자동 제어 시스템, 특히 에너지, 유통, 통신, 수자원을 지원하는 하부구조에 대해 특별히 강조를 하고 있으며 계량기는 이러한 초점에 직접적으로 관련이 있다. 보안은 계량기와 데이터 집중기로부터 회사의 정보시스템에 이르는 계량 과정 전반에 걸쳐 이루어져야 하는데, 여기에는 각 네트워크와 통신(가정망, 공중망, 기업망)에 이용되는 미디어가 포함된다. 또한 모든 요소들이 고려되어야 하며, 전체 보안을 다루어야 하는 필요성이 있다. 제조사로부터 공급자, 관련 규범을 만드는 정부에 이르기까지 모든 파트너가 미래 계량 시스템을 보호하고 경각심을 높이는데 협력하여야 한다.

보안 위협과 치명적 동작으로는 허가 받지 않은 사람으로 인한 정보 접근 또는 수정(침입 또는 불법 변경), 자산의 설정을 변경하거나 전기차단기나 가스 밸브 조작에 의한 고객의 단절 등을 가져오는, 침입자에 의한 의도적인 행동(공중 보건과 신뢰에 대한 손실), 시스템의 요소(계량기, 데이터 집중기, 사무실, 통신 시스템)에 대한 서비스 거부(기능과 보안에 대한 타협 절차를 요구하는, 시스템 가용성에 대한 손실), 프라이버시와 법 제정이 있다. 많은 국가에서 개인적이고 비밀성이 요구되는 정보가 통신 상에서 쉽게 노출되지 않도록, 고객과 사람의 권리를 법으로 보호하고 있으며 그리드 시스템이 정보를 누설하는 수단이 되어서는 안된다. 허가받지 않은 목적지로의 정보 도난과 공개는 어렵게 만들어야 한다.

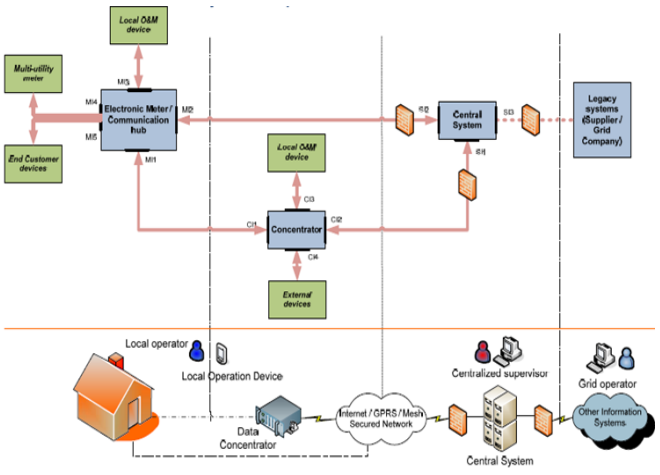

그림 1. OPEN meter 보안 구조(해외사례)

AMI 글로벌 시스템은 허가받지 않은 접근, 기밀 정보의 절도 또는 오용(계량기에 있거나 모든 망을 통해 전달될 때 정보는 읽히거나 수정될 수 없음), 일관성 또는 데이터 처리 및 정보 생성 과정의 안정성 손실, 시스템 가용성의 손실(사무실과 데이터 처리의 보안), 침입과 불법 변경 - 예를 들면 불법적인 펌웨어 업그레이드, 프로세스의 기능에 대한 의심을 초래하거나 시스템 가용량의 손실을 가져오는 절차의 전복(적절한 동작에 대한 책임 분산)을 방지해야 한다. 이러한 필요성을 만족시키기 위해 식별된 요구사항들

로는 접근과 사용자 제어, 데이터 일관성, 데이터 기밀성, 자원 가용성 등이 있다.

AMI 에 대한 일반적인 권고사항은 아래와 같다.

1	시스템은 개체(사용자와 장치)들을 인증할 수 있어야 하고, 각 사용자와 장치를 개별적 또는 그룹 단위로 허용하거나 불허할 수 있어야 함. 이 기능은 모든 AMI 인터페이스(GUI, WAN 인터페이스, 모든 IT 시스템, 데이터 집중기 등)에 적용되어야 함
2	시스템은 적절한 세밀성을 가지고 모든 요소들의 접근 권한을 관리할 수 있어야 함
3	시스템은 중요하다고 식별된 데이터에 대해서는 모든 교환 과정에서의 데이터 일관성을 보장할 수 있어야 함
4	장치는 암호화 키를 포함하는 데이터 저장소의 일관성을 보호할 수 있는 기능을 제공하여야 함
5	장치는 장치 펌웨어의 일관성을 포함한 데이터 저장소의 일관성을 보호할 수 있는 기능을 제공하여야 함
6	시스템과 장치는 도청을 방지하는 기능을 제공하여야 하고, 가능한 가장 안전하고 좋은 암호화 메커니즘을 제공하여 통신과 데이터를 암호화할 수 있어야 함
7	시스템은 재연 방지 메커니즘을 구현할 수 있어야 함
8	시스템의 동작에 대한 감독은 가능해야 하며, 비정상적인 상황은 인지가 되어야 하며, 이에 대한 자동 대응 동작이 가능해야 함
9	장치는 암호화 키를 관리할 수 있는 기능을 제공하여야 함
10	장치에 대한 물리적인 접근은 어려워야 함
11	프로그래밍 디스플레이를 포함한, 사용되지 않는 모든 물리 인터페이스(게이트웨이, 데이터 집중기, 계량기 등)는 애초에 사용불가 상태여야 함
12	장치의 지역 유지보스 포트를 접근하려는 시도는 기록되어야 하고, 설정 간격 동안 대응하는 인터페이스는 사용 불가 상태여야 함
13	IT 기술과 자동화 시스템을 위해 개발된 표준을 존중하는 것이 보호된 AMI 시스템을 구현하는 최선의 방법임. 가능한한 ISO, IEC, NIST, NERC, ISA, IETF 와 IEEE 의 표준을 이용해야 함

3. K-AMI 보안 기능 설계

AMI 권고사항을 바탕으로 한국형 AMI 의 보안 기능을 구축하기 위해 우선, 해외 보안 기술 동향 분석 및 정리를 하였고, 국내 실정에 맞는 AMI 의 기본적인 보안 요구사항, 구간별 요구사항 및 기능 및 종단간 보안 요구사항 및 기능을 설계 하였다.

가) 기본적인 요구사항

① 기본적인 보안 요구사항

K-AMI 시스템이 가져야 할 기본적인 보안 요구사항은 다음과 같다.

1	허가받지 않은 접근, 기밀 정보의 절도 또는 오용(계량기에 있거나 모든 망을 통해 전달될 때 정보는 읽히거나 수정될 수 없음)
2	일관성 또는 데이터 처리 및 정보 생성 과정의 안정성 손실
3	시스템 가용성의 손실
4	침입과 불법 변경
5	프로세스의 기능에 대한 의심을 초래하거나 시스템 가용량의 손실을 가져오는 절차의 전복(적절한 동작에 대한 책임 분산)

이러한 필요성을 만족시키기 위해 식별된 요구사항들은 다음과 같다.

- 사용자와 접근 제어
- 데이터 일관성
- 데이터 기밀성
- 자원 가용성

② 일반적인 권고사항

K-AMI 시스템에 대한 일반적인 권고사항은 다음과 같다.

1	시스템은 사용자와 장치들을 인증할 수 있어야 하고, 각 사용자와 장치를 개별적 또는 그룹 단위로 허용하거나 불허할 수 있어야 하며, 모든 AMI 인터페이스에 적용되어야 함. 따라서 사용자 및 개체를 인증하는 체제 구축이 필요함
2	시스템은 적절한 세밀성을 가지고 모든 요소들의 접근 권한을 관리할 수 있어야 함. IEC-62351-8 에서 소개하고 있는 역할기반 접근제어(RBAC) 기법의 도입이 필요함.
3	시스템은 중요하다고 식별된 데이터의 모든 교환 과정에서 데이터 일관성을 보장할 수 있어야 하며, 따라서 암호화 기능이 반드시 필요함. 이때 영역별, 장치별로 연산 능력 등의 환경 차이가 있으므로, 적절한 수준의 암호화 기능이 선택적으로 이용될 수 있어야 함
4	시스템과 장치는 펌웨어, 암호화 키를 포함하는 데이터 저장소의 일관성을 보호할 수 있는 기능을 제공하여야 함
5	시스템과 장치는 도청을 방지하는 기능을 제공하여야 하고, 가능한 가장 안전하고 좋은 암호화 메커니즘을 제공하여 통신과 데이터를 암호화할 수 있어야 함
6	장치는 암호화 키를 관리할 수 있는 기능을 제공하여야 함
7	시스템은 재연 방지 메커니즘을 구현할 수 있어야 함
8	시스템의 동작에 대한 감독은 가능해야 하며, 비정상적인 상황은 인지가 되어야 하며, 이에 대한 자동 대응 동작이 가능해야 함
9	장치에 대한 물리적인 접근은 어려워야 함
10	프로그래밍 디스플레이를 포함한, 사용되지 않는 모든 물리 인터페이스(게이트웨이, 데이터 집중기, 계량기 등)는 초기에 사용불가 상태여야 함
11	장치의 지역 유지보스 포트를 접근하려는 시도는 기록되어야 하고, 설정 기간 동안 대응하는 인터페이스는 사용 불가 상태여야 함
12	IT 기술과 자동화 시스템을 위해 개발된 정보보호 표준을 수용하여 AMI 시스템 보안을 강화

나) 구간별 요구사항 및 기능 설계

AMI 보안에 대한 요구사항을 도출하기 위하여 우선, 각 구간별로 보안 관련 요구사항을 도출할 필요가 있으며, 따라서 HAN(Home Area Network) 영역과 SUN(Smart energy Utility Network) 영역으로 분리하여 보안 요구사항을 분석할 필요가 있다.

① 인터페이스 및 주요 보안 기능

KEPCO 통합운영센터와 고객측 수용가와의 통신이 이루어지는 전체 구성 및 기능을 아래 그림에 표현하였다. KEPCO 통합운영센터에서는 검침데이터를 수집하고 관리하기 위한 FEP, AMI Server, MDMS가 존재하며 개체인증과 데이터 암호화를 위한 인증서버(Certificate Authority)가 존재한다. 또한 공중망과 연계되기 때문에 안전한 통신을 위한 침입탐지 시스템(IDS)과 방화벽(Firewall)이 존재한다. 고객측 HAN 구간에는 IHD, H-EMS, 스마트미터, 가전기기, 분산전원, 차량용 서브미터가 존재하며 통합운영센터와 HAN 사이에 데이터를 수집하여 올려주는 DCU 가 있다.

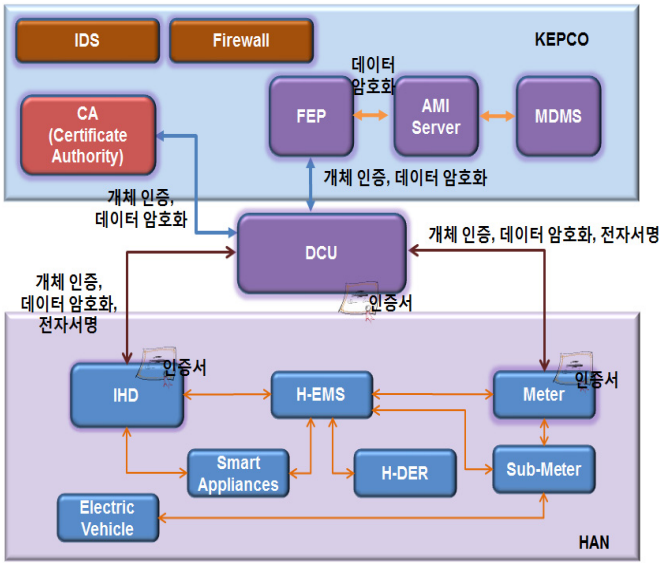

그림 2. AMI 보안 전체 구성 및 기능

② 센터 내에서의 보안 요구사항

일반 공중망이 아닌 기업 전산망 수준의 정보망 보안 구축이 요구된다. 방화벽 및 IDS 를 이용하여 이상 트래픽을 차단하고 역할 기반 접근 제어(RBAC)를 통해 데이터 접근을 제어 해야한다. 또한 감사를 위한 접근 기록을 기록하고 유지하는 것이 중요하다.

③ WAN 구간의 보안 요구사항

DCU 부터 KEPCO 사이의 WAN 구간에서는 VPN 설치를 통해 IPSEC, TLS 등의 기술 적용이 요구되며 개별 DCU 인증을 위해 인증서 기반 관리 체계가 필요하다.

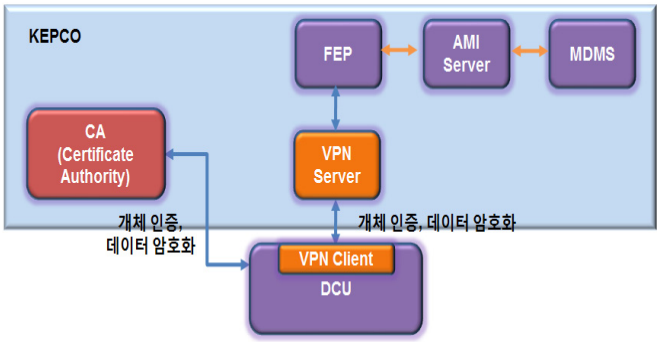

그림 3. WAN 구간 개체 인증 및 데이터 암호화

④ HAN 구간의 보안 요구사항

댁내에서는 IHD, 에너지관리시스템, 스마트미터, 차량 검침용 서브미터, 분산 전원, 스마트 가전기기간 통신이 이루어진다. 댁내의 스마트미터, IHD 와 외부의 DCU 간의 통신이 이루어지는 구간이 HAN 구간이며 안전한 데이터 송수신을 위해 기기 인증서를 사용해 개체를 인증하며 그이외에도 데이터 암호화, 전자서명과 같은 보안 기술이 요구된다.

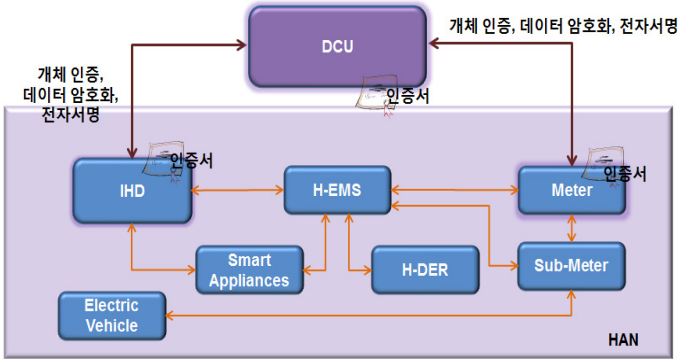

그림 4. HAN 구간의 보안 구성

⑤ DCU-AMI, DCU-IHD 구간

스마트미터와 DCU, 스마트미터와 IDH 간의 통신은 유무선 방식으로 이루어지며 유선방식에는 PLC 기법, 무선 방식에는 ZigBee 방식이 주로 사용된다. PLC 방식의 보안에는 ECC 기반 공개키 암호 알고리즘 또는 ARIA 를 이용한 데이터 암호화 기술을 적용할 수 있고 인증서 기반의 인증이 가능하며 ZigBee 방식의 보안에서는 SE Profile 1.0(키교환: ECC, 암호화:AES128)을 적용 가능하며 마찬가지로 인증서 기반 인증이 가능하다.

다) 종단간 보안 요구사항 및 기능 설계

전력시스템 운영에서의 종단간 보안은 사용자의 인증, 프로토콜 암호화 이상의 것을 요구하고 있다. 종단간 보안은 보안 정책, 접근 제어 메커니즘, 키 관리, 감사 로그, 그 외 정보 하부구조 자체의 보안 문제를 포함하고 있으며 NSM(Network and system management) 데이터 객체 모델에 기반한 종단간 보안 기능 설계가 필요하다. NSM 에 의해서 소프트웨어 응용, 하드웨어 장치, 통신의 상태 감시, 침입탐지, 구

성관리 등의 기능이 제공되며 NSM 표준에서는 운영 환경에서의 통신망과 종단 장치 감시, 통신망과 종단 장치에 대한 제어를 제시하고 있으며 아래 그림과 같이 전력시스템 운영에서 데이터가 지나가는 모든 요소들에서 NSM 객체가 구현되어야만 종단간 보안 기능을 제공할 수 있다. 추가적인 보안을 위해 공개 네트워크와 연결되는 KEPCO 통합운영센터와 DCU 간의 통신구간, DCU 와 HAN 통신구간에 방화벽과 침입탐지시스템을 설치하여 인가되지 않은 사용자의 불법적인 접근을 방지해야 한다.

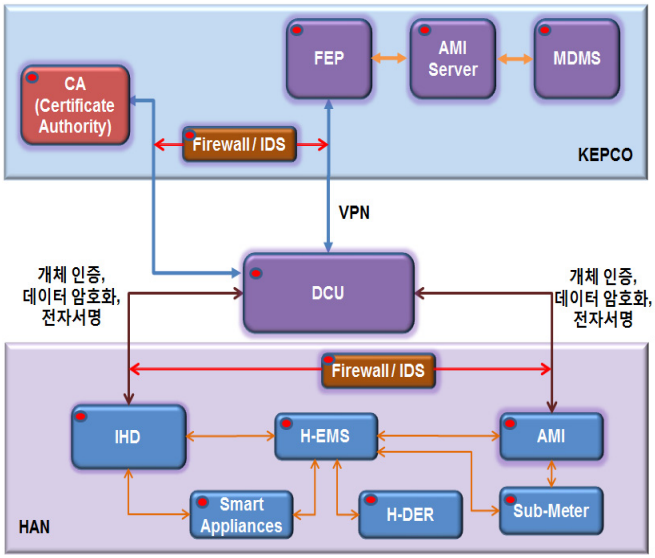

그림 5. 종단간 보안 기능 구현을 위한 NSM 객체와 IDS 위치

4. 결 론

각 요소에서 구현되어야 하는 NSM 객체는 다음과 같다. 먼저 망 구성 감시 및 제어, 망 백업 감시, 통신 장애 및 성능 저하 감시, 통신 프로토콜 감시를 위한 통신 건강 NSM 데이터 객체가 구현되어야 하며 종단 시스템 감시 및 종단 시스템 보안 관리를 위한 종단 시스템 건강 NSM 데이터객체가 필요하다. 다음으로 허가받지 않은 접근 감시, 자원 소진, 버퍼 오버플로우, 변조/기형 PDU, 물리 접근 방해, 비정상적인 망 접근, 협력 공격을 방지하기 위한 침입 탐지 NSM 데이터 객체가 종단간 보안을 위해 구현되어야 한다.

NSM 객체 정의와 구현은 각 요소의 기능과 적용되는 프로토콜을 고려하여 표준화할 필요가 있으며 IEC 62351-3 ~ IEC62351-6 의 표준안을 먼저 적용하고 K-AMI 요소를 정의한 후 IEC62351-7 에서 언급한 NSM 객체들의 표준화를 추진해야 할 것이다.

참고문헌

[1] 김영준외, 스마트그리드 시스템에서의 고객 데이터 공유 및 관리방식 제안, 대한전기학회, 2010.5

[2] Security Profile for Third Party Data Access - The NIST SGIP Cyber Security & The UCAlug SG Security Working Group , 2010.1.

[3] AMI-SEC Task Force,“AMI System Security Requirements – V1.01.”http://osgug.ucaiug.org/utilisec/amisec, 2008.12