스마트그리드와 사이버 보안

이건희 | 서정택 | 이철원
한국전자통신연구원 부설연구소

요 약

스마트그리드는 정보통신 기술과 전력망의 융합으로 탄생한 새로운 형태의 차세대 전력망으로, 전력공급의 중추인 스마트그리드가 사이버 공격에 피해를 입으면 국가 전력마비와 같은 큰 피해를 입게 될 것이다. 실제 최근 전력망에 대한 사이버 공격 위협이 증가하고 있고 실제 공격 사례도 지속적으로 보고되는 등 스마트그리드에 대한 사이버 보안 위협은 간과할 수준의 것이 아니다. 이에 본 논문에서는 스마트그리드에 대한 사이버 보안 위협과 스마트그리드 사이버 보안성 강화를 위한 국내 · 외의 다양한 노력에 대하여 살펴보고, 국내 스마트그리드의 보안성 강화를 위해 향후 서둘러 수행해야 할 사이버 보안 대응 방안을 제시한다.

I. 서 론

스마트그리드란 기존 전력망(발전→송배전→판매)에 정보기술(IT)을 접목하여, 전력공급자와 소비자가 양방향으로 실시간 정보를 교환, 에너지효율을 최적화하는 차세대 전력망이다[1]. 스마트그리드를 통해 에너지를 절약하고, 에너지 생산 비용을 줄이며, 에너지 공급의 신뢰도를 높여 보다 안정적으로 전력을 공급할 수 있다. 스마트그리드는 신재생 에너지의 이용 비율을 높여 지구 환경 문제 극복에 일조하고, 자동화된 송 · 배전을 통해 보다 안정적으로 높은 품질의 전기를 사용자에게 공급하며, 실시간 과금 체계를 통해 사용자에게 요금 절약 효과를 제공할 수 있다.

전기로 인해 동작하는 전자제품 및 기기 설비의 사용이 대다수인 현대사회에서 전력차단은 국가를 일 순간 정지상태로 만드는 것과 같다. 대규모 정전이 발생하면 국민 불안이 증가하고, 생산은 불가해져 생필품 수급은 물론 수출입에 어려움이 발생할 것이다. 따라서 전력망은 현대 사이버 戰에 제1공격 목표가 될 것이다.

스마트그리드는 기존 전력망과 달리 사용자의 참여 증가를 유도하기 위해 사용자와 공급자사이의 빈번한 정보교환이 발생하고, 이를 위해 양방향 의사소통을 위한 통신수단이 구축됨에 따라 이를 통한 다양한 사이버 공격 위협이 발생하고 있다. 따라서 스마트그리드에 사이버 공격이 감행될 경우 현재의 전력망에 비해 보다 쉽게 적의 손에 넘어갈 수 있다. 따라서 안전한 스마트그리드 구축을 위한 사이버 보안 기술의 개발이 필요하다.

지난 2009년 7월 발생한 대규모 DDos 공격은 단순히 특정 웹사이트만을 목표로 했으므로, 웹 페이지 접속불가로 인한 개인불편, 기업의 이미지 실추, 전자거래 중단으로 인한 기업 손실 등 그 피해가 개인 및 사업자에게 국한되었다. 하지만, 그러한 대규모의 공격이 스마트그리드를 목표로 발생한다면, 그로 인한 피해는 국가 안보에 대한 위협으로 까지 발생할 수 있는 중요한 문제다. 실제 미국 에너지부에서 정의한 스마트그리드의 주요 특징 8가지 중 한 가지가 사이버 공격 및 물리적 공격에도 견딜 수 있는 능력이다[2].

본 논문에서는 전력망 및 스마트그리드에 대한 다양한 사이버 공격 사례를 살펴봄으로써 위험에 처한 스마트그리드 현실을 짚어보고, 현재 국내 · 외에서 진행되고 있는 스마트

그리드를 보호하기 위한 사이버 보안 동향을 살펴본다. 또한, 스마트그리드에 대한 사이버 공격 경로를 살펴본다. 마지막으로 본 논문의 말미에서는 스마트그리드를 사이버 공격으로부터 보호하기 위해 필요한 다양한 보안강화 전략을 살펴봄으로써 현재 추진 중인 스마트그리드를 보다 안전하게 구축할 수 있는 방안에 대해 생각해 보도록 한다.

II. 스마트그리드와 보안 위협

1. 스마트그리드

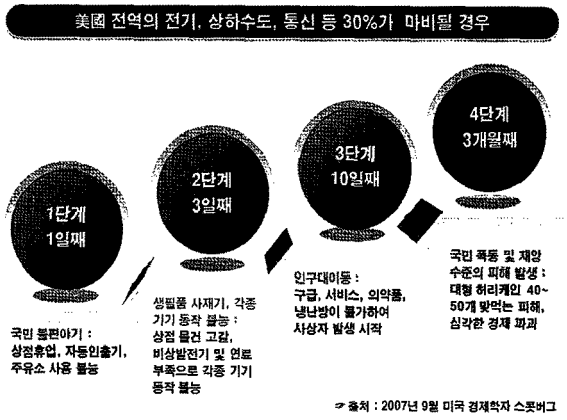
스마트그리드 환경에서는 많은 시스템이 복잡하게 얽혀 서로 협력하면서 동작한다[3]. 스마트그리드가 구축되면 신재생 에너지원 일반화, 그린카 일반화, 사용자의 전기 사용 패턴 변화 등을 통해 산업, 경제, 사회 전반의 변화가 초래된다. 기존에는 전력 공급자에 의한 일방적인 의사소통이 이루어졌지만, 스마트그리드가 완성되면 소비자의 지속적이고 적극적인 참여를 통해, 전력 공급자와 소비자간 유기적인 상호작용에 의해 보다 효율적으로 전력 운영이 이루어진다.

또한 기존 전력망에 비해 전력망과 연결되는 단말장치의 수가 급증한다. 예를 들어, 우리나라 1,500만 가구당 4개의 스마트 가전을 사용할 경우 6,000만개의 단말장치가 스마트그리드에 연결된다.

또한, 전력 공급자와 소비자간의 양방향 정보 교환을 위한 네트워크가 구축되며, 전력 제어시스템은 스마트그리드 환경에서도 계속 전력 생산 · 분배와 관련된 설비의 운영을 제어하는 등의 국내 전력망의 핵심 기능을 수행한다.

2. 증가하는 스마트그리드 사이버 위협

전력시스템은 국가의 기반시설로 사이버침해사고 발생 시 재앙적 수준의 피해가 발생한다. 국가 전력망은 전력 제어시스템에 의해 운영되고 있어, 전력제어시스템이 해커에 의해 침해 당할 경우에는 명령어 변조 공격을 통하여 대규모 정전사태 유발이 가능하다. 美國 경제학자 스콧버그에 의하면, 국가 전력망 1/3의 전력공급이 중단되면 3일째 상점 물건이 바닥나고 연료가 없어 비상발전기 동작이 불가하며, 10일째 인구대이동이 시작된다고 분석했다. (그림 1)은 스콧버그의 시나리오를 도식화 하고 있다[4].



(그림 1) 전력망 마비에 따른 사회 · 경제 파급효과

더욱이 현재의 전력망과 달리 스마트그리드 환경에서는 정보기술이 전력망과 융합되면서 폐쇄망으로 운영하던 전력망이 다양한 정보 시스템과 통신망을 통해서 연결되며, 이러한 연결통로를 통해 사이버 스파이 등 외부 공격자들이 전력망을 장악할 수 있고, 긴급 상황 시 전력망을 공격하여 국가 위기를 조장할 수 있다.

더욱이 국외에서는 최근 스마트그리드 취약점이 지속적으로 보고되고 있다. 다음은 최근 보고된 주요 스마트그리드 보안위협 사례들이다.

- 美國 보안업체인 IOActive사는 스마트 미터를 통하여 스마트그리드를 공격 가능함을 확인[5]
  - 스마트그리드 기기들에 대한 보안성 점검 결과, 해커들이 간단한 해킹기술로 네트워크 접속, 전력 공급도 중단할 수 있음을 확인
- IOActive社의 Mike Davis가 스마트 미터 사이에 자동으로 확산 가능한 웜 바이러스를 소개하고, 웜 전파 시뮬레이션 결과를 발표[6]
  - 스마트 미터에는 원격지에서 전기 공급을 중단시킬 수 있는 기능이 있으므로, 전파된 웜이 일시에 동작하면 지역적인 정전 사태가 발생할 수 있음
  - 시뮬레이션 결과 24시간 만에 15,000 ~ 20,000 가구의 스마트 미터가 감염됨

또한, 다음은 최근 해외 정보기관 수장들이 전력망 및 에너지 산업에 대한 사이버 공격 사례들이다. 이에 의하면 스마트그리드가 사이버戰의 제1목표로 부각되고 있음을 더욱 잘 알 수 있다.

- 미국 CIA 수석 분석가가 러시아와 중국의 사이버스파이가 미국 전력망에 침투했다고 발표[7]
  - 미국의 전력 시스템에 악성 프로그램을 설치했으며, 유사시 미국에 대규모 정전사태를 발생시키는 것이 목적이었다고 발표
- 독일 방첩기관인 헌법수호청(Bundesamt fur Verfassungsschutz)은 러시아가 독일 에너지 산업을 집중 공략하고 있다고 발표

3. 스마트그리드 사이버 보안 위협

(그림 2)는 기존의 전력망과 달리 스마트그리드가 사이버 공격에 더욱 취약할 수 밖에 없는 이유를 설명한다.

(그림 2) 스마트그리드 보안 위협 발생요인

첫째, 스마트그리드에서는 최종 단말 장치와 내부 운영 시스템 사이의 양방향 정보 교환이 필요하게 된다. 스마트그리드는 다양한 정보 수집과 요구 사항 수집을 통해 적절한 전력 수급 및 계통 운영을 자동화하여 수행한다. 또한, 필요에 따라 스마트그리드 운영 시스템에서 최종 단말 장치로 제어 명령 및 정보 제공을 해야 할 필요가 있다. 그러나 일부 노드에서 제공된 잘못된 상태정보 및 상황정보는 해당 지역의 마이크로그리드의 안전에 위협을 가하고, 이는 다시 전체 스마트그리드의 안정성 보장 불가 및 사이버 위협으로 이어질 수 있다는 단점이 이다. 따라서 이러한 문제를 제어할 수 있는 사이버 보안 대책 마련이 시급하다.

둘째, 스마트그리드에서는 사용자 단으로부터 공공 설비로의 접근 경로가 증가하게 된다. 기존의 전력망과는 달리 AMI, DR 등의 시스템으로 인해 전력 수요자와 공공설비 및 제어 시스템 사이의 정보 접점이 존재한다. 수요자단에서 정보교환의 접점이 될 수 있는 스마트 미터, 센서 등의 기기는 보안 관리가 엄격하게 이루어지지 않으므로 공격자의 공격 경로로 활용될 수 있다. 특히 이러한 기기들은 전국 곳곳에 산재하므로 일일이 개별적으로 위험관리 및 보안관제를 하는 것이 불가능하다.

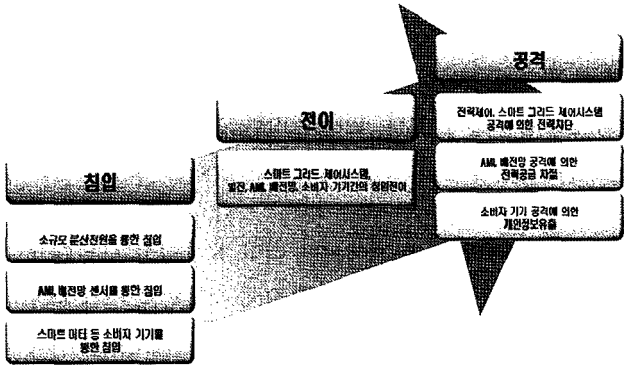
셋째, 스마트그리드 환경에서는 이미 개발되어 사용되고 있는 상용기술을 스마트그리드 환경에 적합하게 수정하여 사용하는 경우가 증가할 것이다. 특히 통신 기술 및 소프트웨어 기술 등이 이에 해당한다. 이를 통해 스마트그리드는 보다 쉽게 구축될 수 있지만, 상용 정보통신 기술에 현존하는 다양한 사이버 보안 위협이 곧 스마트그리드에서의 사이버 보안 위협으로 이어질 수 있는 문제는 피할 수 없다.

넷째, 스마트그리드 역시 정보기술이 복합된 전력망의 일종이므로 반드시 제어 시스템이 포함되어야 한다. 스마트그리드는 기존의 전력망과는 달리 중앙집중 방식 운영이 아닌 분산된 운영 구조를 지닌다. 따라서 마이크로 그리드를 위한 제어시스템, 배전을 위한 제어시스템, 송전을 위한 제어시스템 등 다양한 환경에 대한 제어시스템이 존재해야 한다. 그러나 현존하는 대부분의 제어시스템은 정보보안에 대한 고려가 부족하게 개발되었고, 이로 인해 다양한 보안 취약점을 내재하고 있어 보안 위협이 크다. 지속적으로 보고되고 있는 전 세계 다양한 제어시스템 해킹 관련 사례 발표[8], 보안 기술 연구[9][10][11], 취약점 보고[12] 등이 이를 뒷받침한다.

III. 스마트그리드 사이버 공격 시나리오

스마트그리드 환경이 되더라도 발전, 송전, 변전, 배전과 관련된 핵심 기능은 모두 제어시스템 및 운영시스템이 담당

하게 된다. 따라서 정전 등의 가장 위협적인 피해를 입히는 사이버 공격을 실행하기 위해서는 결국 제어시스템 또는 운영시스템과 같은 중요 시스템을 장악하여 조작하는 것이 될 것이다. 이러한 관점에서 본 논문에서는 스마트그리드에 대한 사이버 공격 시나리오를 (그림 3)과 같이 구성해 보았다.



(그림 3) 스마트그리드 침입 시나리오

스마트그리드를 장악하기 위해서는 우선 가장 접근이 용이한 스마트그리드 단말기기를 공격해야 한다. 스마트그리드 단말기기는 각 시스템의 최종단에 설치되어 각 정보 수집 및 장치 제어 등을 담당하는 간단한 기기로 송·배전망 감시를 위한 센서, AMI 최종 단말로 각 가정에 설치될 스마트 미터 등이 이에 해당한다. 이러한 단말기기는 공격자의 접근을 막기 위한 보호 장치가 거의 없고, 외부자가 쉽게 접근할 수 있는 외부에 설치되므로 공격에 매우 취약하다. 이와 더불어 소규모 분산 전원의 경우 물리적 보안관리가 소홀히 이루어지고 있어, 이를 통해 스마트그리드 핵심 시스템으로 침입할 수 있다.

단말기기 및 분산전원을 통해 일단 스마트그리드 네트워크로 침입한 공격자는 이후 중앙 제어시스템 또는 운영시스템의 취약점을 이용해 스마트그리드를 장악하게 된다. 제어시스템 및 운영시스템에는 다양한 소프트웨어가 설치되어 운영되고 있으며, 이러한 소프트웨어는 여러 취약점을 가진다.

이렇게 스마트그리드 주요 시스템으로 침입에 성공한 공격자는 제어시스템을 통해 전력차단, 개인정보 유출 등의 공격을 시도하고, 이를 통해 피해를 유발할 수 있다.

Ⅳ. 국내 · 외 스마트그리드 사이버 보안 동향

1. 국외 스마트그리드 사이버 보안 동향

미국은 정부차원에서 스마트그리드에 대한 사이버 보안에 대해 큰 관심을 보이고 있다. 미국은 지난 2007년 제정된 에너지 독립 및 안보법(Energy Independence and Security Act of 2007)에서 스마트그리드 추진에 대한 법률을 제시하였는데, 이 법안에서는 사이버 공격에 대한 대응 능력을 스마트그리드의 주요 기능 중 하나로 명시하였다[13]. 또, 2009년 4월 미국 상 · 하원 국토안보위원회는 전력인프라보호법(Critical Electric Infrastructure Protection Act)을 발의하여 전력인프라 사이버 침해에 대한 대응 체계를 제시하였다[14]. 이 법안에서는 연방에너지규제위원회(FERC: Federal Energy Regulatory Commission)에 전력 인프라의 사이버보안 관련 긴급 명령 및 제재 권한을 부여하고, 사이버보안 위협에 대응하기 위한 임시 표준을 정립하도록 요구하였으며, 미국 국토안보부에 연방 소유의 중요 전력인프라가 외부로부터 침입되었는지를 알아내기 위한 조사 권한을 부여하였다.

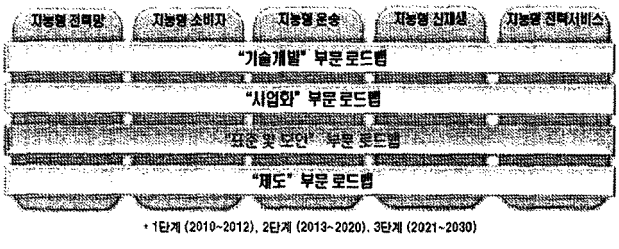
또한 미국 의회는 국립표준기술원(NIST: National Institute of Standards and Technology)을 통해서 스마트그리드의 모든 시스템이 상호운용될 수 있도록 하기 위한 표준을 제시하도록 하였으며, 이에 대한 결과물로 국립표준기술원에서는 스마트그리드 상호운용성을 위한 표준 로드맵 1차 버전을 2009년 9월 발표하였다[3]. 이 로드맵에 포함된 표준들 중 8개의 표준이 사이버 보안 표준이다. 더불어, 스마트그리드 전 영역에 걸쳐 사이버 보안 문제를 고려하기 위해 사이버 보안 워킹 그룹을 별도로 운영하고 있으며, 2010년2월 스마트그리드에 대한 사이버 보안 요구사항을 정립하기 위한 스마트그리드 사이버 보안 전략 및 요구사항에 대한 보고서를 발표하였다[15].

더욱이, 미국 에너지부의 지원을 받아 스마트그리드 시범사업을 진행하기 위해서는 반드시 각 기술에 대한 사이버 보안 대책을 수립하고 이를 검증할 수 있는 방안을 제시하도록 되어 있다. 이에 따라 현재 모든 스마트그리드 구축을 위한 프로젝트들이 사이버 보안 대책을 수립하기 위해 노력하고 있다.

유럽에서도 스마트그리드 유럽기술플랫폼 프로젝트에서 2006년부터 2008년까지 스마트그리드 비전 및 향후 연구개발 전략을 수립했다. 이 연구에서는 5개 연구부분에 19개 세부과제를 선정하였으며, 세부과제 중 하나로 "운영 · 복구, 방어 계획을 위한 아키텍처와 도구"를 선택하였으며, 이 과제에서는 스마트그리드의 장애 및 외부 공격 대응 방안 연구와 송 · 배전 시스템의 사이버 보안 및 복구 능력 향상을 위한 방법론을 연구하는 것을 목표로 하고 있다. 또한 EU 주도로 진행하고 있는 OPENmeter 프로젝트에서는 2009년 7월 보안요구사항을 포함하는 스마트 미터링 명세서를 발표했다. 이는 스마트그리드를 구성하는 중요 인프라인 AMI의 핵심 구성요소인 스마트 미터와 통신 인프라에 대한 보안 요구사항을 제시하고 있다[16].

2. 국내 스마트그리드 사이버 보안 동향

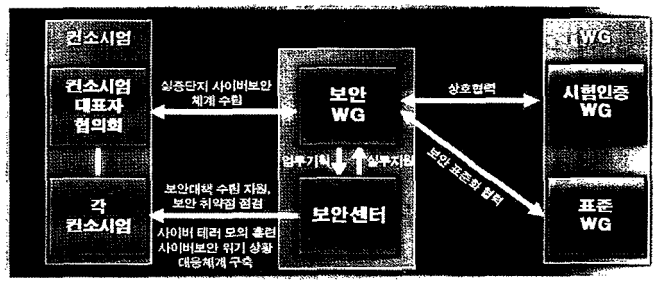
현재 국내에서도 스마트그리드 사이버 보안에 대한 고려가 서서히 진행되고 있다. 우선 2010년 1월 발표된 스마트그리드 국가 로드맵에서는 스마트그리드 구축을 위한 5개 사업 영역의 사이버 보안 강화를 위해 각 영역 별로 스마트그리드 사이버 보안 실행계획이 포함되어 있다[17]. 로드맵에서는 스마트그리드의 안전한 구축을 위한 보안 가이드라인을 2010내에 마련하고, 국가단위의 스마트그리드에 적합한 보안 체계를 2011년까지 마련하도록 하고 있으며, 스마트그리드 보안성 유지를 위한 보안 인증 제도를 운영하도록 하고 있다. 또한 (그림 4)와 같이 각 사업 영역 별로 새롭게 개발해야 할 보안 기술의 단계적인 개발도 명시하고 있다.



(그림 4) 스마트그리드 국가 로드맵

또한 연내에 공표될 스마트그리드 활성화를 위한 법률에 사이버 보안과 관련된 내용을 포함시킬 예정이다. 이 법률에서는 전력망 보안체계를 수립하기 위해서, 국가 안보 관점의 보안 관제 체계를 확립할 것을 종용하고, 기기 및 인프라의 보안관리 체계 수립하여 보다 안전하게 스마트그리드를 관리하고자 한다.

더불어 현재 추진 중인 제주 스마트그리드 실증단지에서 각 시스템에 대한 보안 문제 해결을 위한 노력을 기울이고 있다. 제주 실증단지는 국내 스마트그리드 기술을 시험 · 평가하기 위해 제주도 내 구좌읍에 구축되는 시범사업 단지다. (그림 5)는 실증단지 사이버 보안을 위한 각 조직의 역할을 설명하고 있다.



(그림 5) 스마트그리드 실증단지 보안대책 추진체계

현재 로드맵에서 제시한 5개 사업영역에 해당하는 스마트그리드 시스템을 시범 구축하기 위해 참여한 각 컨소시엄이 자체적으로 사이버 보안 대책을 마련하고, 사업을 주도하는 스마트그리드 사업단에서는 국가보안기술연구소를 통해 보안센터를 운영하고 있다. 보안센터는 각 컨소시엄이 마련한 보안대책에 대한 검토를 수행하며, 실증단지 시스템 구축을 위한 사이버 보안 가이드라인을 제정하고, 실증단지 시스템 및 네트워크에 대한 취약점 분석과 사이버 모의 훈련을 통해 실증단지 사이버 보안성 강화를 위한 업무를 수행한다. 이와 더불어 실증단지 전체의 사이버 보안 체계를 구축한다.

V. 스마트그리드 사이버 보안 대응 전략

이처럼 스마트그리드에 대한 사이버 침해 위협이 증가하

고 있는 상황에서 스마트그리드 사이버 보안에 대한 노력은 더 이상 선택이 아닌 필수가 된 상황이다. 더욱이 앞서 언급한 중국, 러시아 스파이들의 미국 전력망에 대한 공격 사례에서 보듯 스마트그리드는 사이버戰의 주요 목표가 될 것이다.

이러한 상황을 통해 볼 때, 현재까지 국내 전력 제어시스템 및 전력 운영시스템에 대한 사이버 공격 피해사례는 발생하고 있지 않지만, 전력 제어시스템 및 운영시스템을 포함한 스마트그리드에 대한 보안은 시급히 이루어져야 할 것이다. 스마트그리드에 대한 사이버 보안은 그 구축단계에서부터 고려해야 하며, 이를 통해 향후 다양한 사이버 공격으로부터 스마트그리드를 안전하게 보호함으로써, 스마트그리드가 우리의 삶에 긍정적인 영향을 끼칠 수 있도록 해야 한다.

이를 위해서 가장 우선적으로 국가 에너지 사이버안전 체계를 구축해야 한다. 국가 에너지보안 전문위원회를 구성하여 스마트그리드를 포함한 국가에너지에 대한 사이버 보안 정책을 수립하고, 스마트그리드와 관련된 다양한 법안 정리 작업을 수행해야 한다. 법안 정비 작업에서 우선적으로 수행해야 할 작업은 전력 제어시스템 및 운영시스템의 주요정보통신기반시설 지정 의무화 추진이다. 이를 통해 스마트그리드의 주요 시스템이 국가의 집중적인 감독 및 관리를 통해 안전하게 보호될 수 있도록 해야 한다. 이는 곧 향후 스마트그리드를 법 · 제도에 따라 체계적으로 관리하는데 큰 역할을 할 것이다.

또한 스마트그리드에 사용되는 하드웨어 및 소프트웨어에 대한 보안성 평가 및 인증을 의무적으로 받도록 법제화해야 한다. 다양한 업체에서 스마트그리드에 대한 소프트웨어 및 하드웨어를 만들고 서둘러 설치하면 반드시 보안을 고려하지 못하거나 잘못 고려하여 부족한 점이 발생할 수 있다. 따라서 제품을 실제로 사용하기 전에 소프트웨어 및 하드웨어의 보안성을 검토하고 이를 공인된 인증기관을 통해 인증받도록 하여, 안전하다고 검증 받은 기기 및 소프트웨어만을 사용함으로써 스마트그리드 전체의 보안성을 향상시킬 수 있도록 해야 한다.

보안성 평가와 유사한 맥락에서 스마트그리드 연구개발과제에 대한 보안성 검토 제도를 마련해야 한다. 스마트그리드 연구개발 시 초기에 설계된 시스템의 보안성을 검토하여 향후 보안 취약점으로 인한 문제 발생 가능성을 최소화할 필요가 있다. 이런 보안성 검토 과정은 개발 과정 전반에 걸쳐 지속적으로 수행될 수 있어야 하겠다.

이러한 정책적인 대안과 더불어 새로운 기술 개발도 병행되어야 하겠다. 그 중에 가장 우선적으로 개발되어야 하는 기술은 전력 제어시스템 보안기술이다. 스마트그리드 환경에서 전력 제어시스템이 차지하는 중요성과 다양한 사이버 공격이 계속 보고되고 있는 사실과, 국제적으로 전력 제어시스템에 대한 보안성 요구가 높아지는 국제 동향을 고려할 때 시급히 전력 제어시스템 보안을 강화하기 위한 국가적 차원의 보안기술 연구개발이 추진되어야 한다. 현재 진행중인 전력 제어시스템 연구개발 과제의 경우에는 지금부터라도 당장 보안을 고려하여 보안대책을 마련할 필요가 있다.

이와 더불어 스마트그리드에 대한 사이버 보안 기술의 연구개발을 수행해야 한다. 스마트그리드는 현재 실증단지 조성을 통해 새로운 서비스와 기술을 실증하는 단계에 있고, 실증하기 위한 다양한 기술을 여러 연구기관 및 기업에서 서둘러 개발하고 있다. 따라서 지금과 같은스마트그리드 구축 시작 단계에서 사이버 보안을 고려한다면, 향후 발생가능 한 여러 문제점을 차단할 수 있도록 미리 준비할 수 있다. 만일, 구축 완료 후 필요에 따라서 보안성을 강화 한다면, 이를 위해 시스템 변경 및 구조 변경을 해야 하는 등 막대한 비용이 필요하게 된다.

마지막으로, 스마트그리드의 사이버 보안성 강화 추진을 위한 보안 협의체를 구성할 필요가 있다. 국민의 생명 · 안전, 국가 안보 등과 밀접한 관계가 있는 국가 제어시스템을 주 대상으로 한 보안 협의체를 설립하여 스마트그리드 보안을 위한 정책이슈 개발 및 법 · 제도적 개선사항을 발굴하는데 협력해야 할 것이다. 이 협의체에는 산 · 학 · 연 · 관 전문가가 모두 참여하여 국가 스마트그리드 사이버 안전 문제에 대한 공감대 형성 및 안전전략 수립 등에 대해 지속적인 의견교류를 추진해야 할 것이다.

VI. 결 론

스마트그리드는 양방향 통신, 정보기술 등을 이용하는 차세대 전력인프라로, 기후변화 개선, 에너지 효율성 향상, 新산업 발전 등에 도움을 줄 수 있다. 하지만 스마트그리드가 사이버 공격을 통해 침해를 당하면 작게는 국지적 정전, 크게는 국가 차원의 정전으로 이어질 수 있어 큰 피해가 예상된다. 실제 전력망에 대한 공격 시도는 지속적으로 증가하고 있어 차후 사이버戰에서는 스마트그리드가 제 1 공격목표가 될 것이다.

이에 미국, 유럽 등의 스마트그리드를 추진하는 국가들은 모두 사이버 보안 강화에 큰 노력을 쏟고 있다. 국내에서도 스마트그리드의 사이버 보안 강화를 고려하고는 있지만, 그 노력의 상대적 크기가 매우 작은 상황이다. 따라서 국내 스마트그리드의 안전을 위해 스마트그리드 보안 강화 노력에 박차를 가해야 하겠다. 이를 위해 본 논문에서는 크게 네 가지 방안을 제시하였다. 첫째, 법 제도 개선을 통해 국가 에너지 사이버안전 체계를 구축하여 위기 상황에 대한 예방 및 대처를 위한 체계를 마련해야 한다. 둘째, 스마트그리드 기기 및 소프트웨어에 대한 보안성 평가 및 인증을 의무화해야 한다. 셋째, 정책 및 제도 개선과 더불어 스마트그리드 보안성 강화를 위해서 각 분야별 필요 보안 기술을 서둘러 연구 · 개발해야 하겠다. 마지막으로 넷째, 스마트그리드 보안을 위한 사이버 보안 협의체를 운영하여야 하겠다. 본 논문에서 제시된 방향이 스마트그리드를 보다 안전하게 보호하여 국가안보 능력 향상에 큰 기여를 할 수 있을 것으로 기대된다.

참 고 문 헌

[1] F. Sissine, "Energy Independence and Security Act of 2007: A Summary of Major Provisions", CRS Report for Congress, Dec. 2007.

[2] NETL, "A Vision for the Modern Grid", The NETL Modern Grid Initiative, National Energy Technology Laboratory, Mar. 2007.

[3] U.S. National Institute of Standards and Technology, "NIST Smart Grid Framework 1.0 document", NIST Special Publication 1108, Sept. 2009.

[4] "Staged Cyber Attack Reveals Vulnerability in Power Grid", CNN News, 2007. (http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html)

[5] "Smart Grid May be Vulnerable to Hackers", CNN News, 2009. (http://www.etnews.co.kr/news/detail.html · id=200903240003)

[6] Mike Davis, "Smart Grid Device Secuiry - Advantures in a New Medium", Blackhat USA 2009, July 2009.

[7] "Electricity Grid in U.S. Penetrated By Spies", Wall Street Journal, 2009. (http://online.wsj.com/article/SB123914805204099085.html)

[8] M. Abrams, J. Weiss, "Malicious Control System Cyber Security Attack Case Study · Maroochy Water Services, Australia", Report, NIST Computer Security Division, Aug. 2008.

[9] Juniper Networks Inc., "Architecture for Secure SCADA and Distributed Control System Networks", White Paper, Feb. 2009.

[10] Y. Wang, B.T. Chu, "sSCADA: Securing SCADA Infrastructure Communications", Cryptology ePrint Archive, Aug. 2004.

[11] R.J. Robles, M. Choi, E. Cho, S. Kim, G. Park, S. Yeo, "Vulnerabilities in SCADA and Critical Infrastructure Systems", International Journal of Future Generation Communication and Networking, pp.99-104, Dec. 2008.

[12] US-CERT, "Control Systems Security Program - Vulnerability Notes", 2009. (http://www.us-cert.gov/control_systems/csdocuments.html)

[13] US Congress, "Energy Independence and Security Act

of 2007", 2007.
(http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi · dbname=110_cong_bills&docid=f:h6enr.txt.pdf)

[14] US Congress, "Critical Electric Infrastructure Protection Act", 2009.
(http://www.govtrack.us/congress/billtext.xpd · bill=s111-946)

[15] SGIP-Cyber Security Working Group of U.S. National Institute of Standards and Technology, "Smart Grid Cyber Security Strategy and Requirements", Draft NISTIR 7628, Feb. 2010.

[16] G. Romero et al., "Report on the Identification and Specification of Functional, Technical, Economical and General Requirements of Advanced Multi-Metering Infrastructure, Including Security Requirements", The OPENmeter Consortium, 2009.

[17] 지식경제부, "스마트그리드 국가로드맵", 지식경제부, 2010.
(http://www.smartgrid.or.kr/09smart2-6-1.php)

약 력

이 건 희

2001년 아주대학교 정보및컴퓨터공학부 (학사)
2003년 아주대학교 정보통신전문대학원 정보통신공학과 (석사)
2009년 아주대학교 정보통신전문대학원 정보통신공학과 (박사)
2009년 ~ 현재 한국전자통신연구원 부설연구소 연구원
관심분야 : 제어시스템 보안, 스마트그리드 보안, 무선 네트워크 보안, 표준

서 정 택

1999년 충주대학교 컴퓨터공학과 (학사)
2001년 아주대학교 컴퓨터공학과 (석사)
2007년 고려대학교 정보경영공학전문대학원 정보보호전공 (박사)
2001년 ~ 현재 한국전자통신연구원 부설연구소 선임연구원 / 과제책임자
관심분야 : 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응

이 철 원

1987년 충남대학교 수학과 (학사)
1989년 중앙대학교 전자계산학과 (석사)
2009년 아주대학교 컴퓨터공학과 (박사)
1989년 ~ 1994년 한국전자통신연구원 선임연구원
1994년 ~ 2000년 한국정보보호진흥원 선임연구원 / 과제책임자
2003년 ~ 2004년 Texas A&M University 방문연구원
2001년 ~ 현재 한국전자통신연구원 부설연구소 책임연구원 / 본부장
관심분야 : 사이버 안전, 정보보호시스템 평가, S/W 안전성 분석, 산업보안 등