스마트그리드 보안 위협 및 전략

임용훈〈전력연구원 선임연구원〉

1. 서 론

스마트그리드는 '발전-송전·배전-판매'의 단계로 이루어지던 기존의 단방향 전력망에서 전력과 ICT 정보기술을 융합하여 전력 공급자와 소비자가 양 방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형 전력망이다. 하지만, 이런 스마트그리드는 양방향 정보 전송이 가능하고 개별 사용자의 정보 또한 전달되기 때문에 개인정보 보호를 비롯한 스마트그리드 보안의 중요성이 크게 증가하고 있다. 과거 폐쇄적이던 전력망 운용 데이터 통신 구조가 연결 개소의 확대와 상용 S/W 사용 그리고 공개된 표준 통신 프로토콜을 사용함으로써 일부 개방된 구조로 패러다임이 변화됨으로 인해 정보통신기술이 지닌 부작용이라 할 수 있는 해킹 등의 사이버 공격과 개인정보 유출 같은 잠재적인 보안위협에 노출될 가능성이 높아 질 수 있다. 실제로 스마트그리드에 대한 사이버 공격 위협은 해외의 몇 몇 사례를 통해서 얼마나 현실적인 위협으로 여겨질 수 있는지 가늠할 수 있다. 스페인에 설치된 800만대(전체 가구의 30%)의 스마트미터는 적절한 보안대책을 갖추고 있지 못해 원격에서 검침정보 조작이나 전력 차단이 가능하고 악성코드에 감염된 스마트미터로 인해 대규모 블랙아웃 공격이 가능하다고 지난 2014년 로이터 통신을 통해 보도된 바 있다. 2012년 서인도제도에 위치한 미국 자치령 푸에르토리코에서는 스마트미터의 취약점을 통한 전력 사용량 조작 사고로 연 4억 달러 규모의 현실적인 피해를 입혔다고 FBI가 발표하기도 하였다.

2. 스마트그리드 보안위협

2.1 배 경

기존 전력계통그리드는 발전원에서 소비자(산업, 상업, 일반사용자)에게 전송되는 중앙 집중식 형태인 벌크 파워시스템(Bulk Power System)이였으나 스마트그리드나 마이크로그리드 같은 지능형 전력망기술은 그리드의 운영에 있어 네트워크화 된 제어시스템들(Control Systems)간의 양방향 통신을 통해 전력설비의 상태를 정확히 인지하여 손상된 그리드 요소들을 빠른 복구하거나 경로 절체(Path-Reroute)를 통해 그리드의 안정성(Reliability)과 복구(Resiliency) 성능을 향상 시킬 수 있을 것으로 기대하고 있다.

이것은 기존에는 그리드에 연결되지 않았던 많은 장치들이 측정과 제어를 목적으로 물리적이던 논리적이던(사이버적) 그리드와 연계되고 이러한 연계점이 기하급수적으로 증가되어 기존 전력 회사에 소속된 직원들만 지켜야할 그리드 보안 규제들이 앞으로는

전력설비(또는 스마트그리드) 제조사나 소비자들도 또한 준수해야 되는 대상이 된 다는 것을 의미하기도 한다.

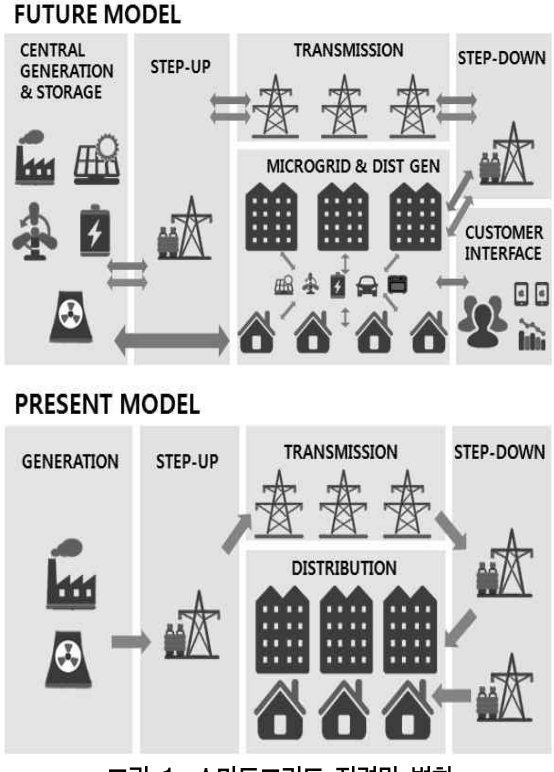


그림 1. 스마트그리드 전력망 변화
(출처 : "Securing the US Electrical Grid")

2.2 송·배전망 사이버 보안위협 사례

유틸리티 회사가 자동화를 목적으로 사용하고 있는 스카다(SCADA : Supervisory Control & Data Acquisition)시스템은 네트워크를 통해 데이터를 수집하고 분석할 수 있어 특정 그리드 요소들을 자동화할 수 있었다. 1920년대에 초기 시스템들이 설치된 이후 1960년대부터 대량 보급되어 급속도로 확산되었다. 이후 스카다시스템은 다양한 개발 세대를 지나 최근에는 시스템 아키텍쳐 플랫폼과 개방된 표준 그리고 통신 프로토콜을 사용함으로써 근거리 통신망(Local Area Network)에서 뿐만 아니라 광역통신망(Wide Area Network)을 이용한 분산 스카다 시스템 구성까지도 가능하게 되었다. 이러한 분산 스카다 기술은 메터링 기술과 소비자와의 인터페이스 기술을 통해 스마트그리드로 발전할 수 있는 기초가 되었다. 분산 스카다시스템은 안전한 스카다 운영이 보장될 수 있도록 어플리케이션 보안, 침입탐지시스템, 물리적 접근통제와 같은 보안 설비 사용을 요구했을 뿐만 아니라 지진, 번개와 같은 외부의 환경재난 위협으로부터 피해를 완화시킬 수 있도록 낙뢰 보호장치(TVSS)와 같은 별도의 센서를 설치하고 안전한 스카다 운전에 필요한 외부인의 엄격한 물리적 접근통제 환경을 요구해 왔다. 하지만 스카다시스템이 물리적으로 안전한 지역에 설치되어 있더라도 보안을 손상시킬 수 있는 위협들은 여전히 존재한다. 내부자 또는 권한이 없는 직원이 시스템에 접근하여 위험(Risk)에 빠뜨릴 수 있는 악성코드에 감염된 USB나 key logger 같은 위협(Threat) 요소들을 설치할 수 있다. 이러한 위협들은 시스템을 즉시 감염시킬 수 도 있고 공격자에게 "back-door"(비정상적인 접근)를 제공함으로써 전체 스카다시스템에 위협을 가할 수 있는 사이버공격 기회를 가능하게 한다. 대표적인 사이버 위협으로는 서비스 거부, 데이터 가로채기, 권한이 없는 사용자의 접근, 자료 교체, 제어 명령어 재전송 등을 들 수 있으며 이러한 위협들로 인해 수백만 명의 고객이 직접적으로 정전 피해를 받을 수 있고, 교통과 통신 그리고 방송국 같은 다른 중요한 인프라 기능을 방해하거나, 중요한 자료들을 탈취 할 수 있게 한다. 사이버 해킹기술이 점점 더 진보되면서 컴퓨터시스템에 가해지는 공격은 빈도, 강도, 다양성 등 모든 면에서 증가하고 있고 'drive-by-shooting'처럼 특정한 공격을 통해 전략적으로 목적 달성에 활용하기도 한다. 현재 CVE(Common Vulnerabilities and Exposure)[1]에 공개된 SCADA와 관련된

취약점은 500개 이상이며 2007년 3월 7일 최초로 오스트리아 자동화 소프트웨어 회사인 NETxAutomation 사의 NETxEIB OPC Server에 원격 코드를 실행하거나 서비스거부를 할 수 있는 취약점이 발견된 이후 2010년 스턱스넷(Stuxnet) 발견을 기점으로 폭발적으로 증가하고 있는 실정이다.

그림 2. 연도별 CVE SCADA 취약점 발생 건수

스턱스 넷(Stuxnet)

지금까지 세계적으로 중요 시설에 상당한 피해를 주었던 여러 바이러스들(악성코드)은 스카다시스템을 목표로 특별히 제작되었다. 2010년 6월 이란에서 발견된 스턱스 넷(Stuxnet) 바이러스는 이란의 핵 시설에 대한 사이버 공격을 목적으로 제작 되었지만 전 세계에 걸쳐 100,000개 이상의 컴퓨터를 감염시킨 것으로 보고되었다. 스턱스 넷은 HMI 소프트웨어로부터 명령어를 가로채서 Simens Simatic WinCC SCADA시스템을 공격하도록 고안된 특정 코드를 가지고 있어 모터를 제어하는 고속 주파수변환기로 보내지는 명령어를 가로채는 Man-in-the-Middle 공격 형태를 보였다.

플레임(Flame)

2012년 5월 발견된 플레임(Flame) 바이러스는 사이버 사보타주 형태의 대표적인 사이버 공격으로 이란의 SCADA시스템을 손상시키기 위한 목적이 있는 것으로 보인다. 이 악성코드는 이란 오일관련 정부조직과 오일회사를 공격 목표로 삼고 HMI 기능과 관련된 제어와 수행하는 업무를 복제함으로써 컴퓨터 네트워크를 감시하고자 계획된 것으로 알려졌다. 플레임은 키보드 로그(log keyboard stokes); 스크린 샷 촬영; 마이크와 카메라를 활성화; 명령어와 자료를 블루투스 기술을 통해 주고 받을 수 있게 고안되었다. 이 스턱스 넷과 플레임 바이러스는 SCADA를 공격 목표로 하는 사이버 공격 가능성을 현실적으로 입증한 사례가 되었다.

에너제틱 베어(Energetic Bear)

아주 최근에, 미국과 유럽의 그리드 인프라가 "드래곤플라이(Dragonfly)"로 알려진 러시아 해커 집단으로부터 공격을 당했다. 2011년부터 프랑스, 이탈리아 등 유럽지역과 미국 에너지기업을 대상으로 지속적인 사이버 스파이 활동이 있었던 사실이 최근 포착되었다. 드래곤플라이의 공격 대상은 주요 발전 업체와 석유 공급 업체, 에너지 산업 장비 업체들과 같은 에너지 관련 기업들에 중점 되었다. 가장 특징적인 공격 활동은 산업제어시스템(ICS : Industrial Control System) 장비 공급업자(제조사)들의 시스템에 침투하여 소트프웨어를 원격에서 접속 할 수 있도록 '트로이 목마'를 감염시키는 것이다. 해커들은 2개의 Remote Access Trojans (RAT)를 이용하여 감염된 컴퓨터에 대한 접근과 제어가 가능한 "에너제

1) CVE : 미국 비영리 연구 단체인 MITRE에서 운영하며, 알려진 보안 취약점에 대한 정보와 조치방법 등을 제공. 취약점 정보는 효과적인 관리를 위해 식별번호(CVE Identifier)로 관리되며 CVE 식별번호는 CVE-연도-발견순서(예 : CVE-2014-3456)로 부여됨.

틱 베어(Energetic Bear)"라고 하는 멀웨어를 설치하고 실행 가능한 파일을 감염된 컴퓨터에 실행시켜 해킹에 필요한 부가적인 플러그인을 설치함으로써 스크린샷을 찍고 감염된 컴퓨터의 문서 목록을 만들면서 훔친 데이터를 추출하고 업로드 할 수 있도록 했다. 드래곤플라이는 ICS 소프트웨어 업데이트 사이트를 감염시키는 것은 물론, 스피어 피싱, 스팸 이메일, 워터링 홀(Watering hole) 기법을 이용하여 공격 목표 조직에 위해를 가할 수 있다. 이를 통해 목표 기관이나 단체의 네트워크를 교두보로 사용할 수 있을 뿐만 아니라 감염된 ICS컴퓨터에 파괴행위를 수행할 수 있다.

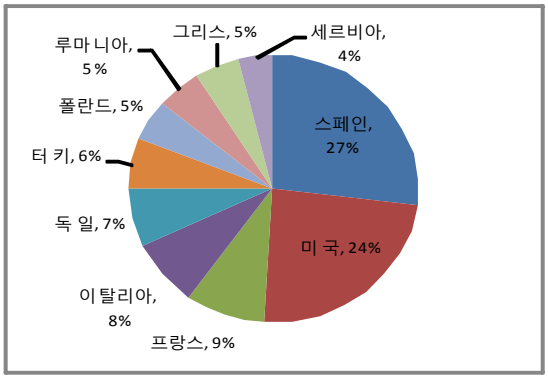


그림 3. 에너제틱 베어에 감염된 상위 10개 국가

2.3 물리적 보안위협 사례

스마트그리드와 같은 지능형 전력망이 당면한 위협들은 사이버 공격, 물리적 보안위협, 전자기파 공격(Electromagnetic pulse, EMP) 등 여러 위협들에 노출되어져 있다. 특히 넓은 지역에서 분산된 그리드 구조상 물리적 공격에 특히 취약하다. 또한 그리드의 특성상 주요 노드에 대한 작은 공격이나 위협들이 일부분의 손상으로도 전체 그리드에 대해 당초 의도했던 것 보다 연쇄적인 효과를 초래함으로써 넓은 지역까지 피해를 일으킬 수 있다. 송변전 설비나 배전설비는 지역적으로 멀리 떨어진 외곽지역에 위치해 있어 관리 인력이 없이 담장과 감시 카메라에 전적으로 의존하고 있다. 지난 2013년 4월 미국 캘리포니아 주 산호세(San Jose) 근교에 있는 PG&E 전력회사의 메트칼프(Metcalf) 변전소에 가해진 총격으로 17개의 변압기가 치명적인 손상을 입게 되었고 시설 복구에만 거의 한 달 가까운 시간이 필요로 하였다. 고속도로 근처에 위치한 변전소에 가해진 총격은 감시 카메라에 기록되었지만 공격자를 찾는 데 실패하였다. 메트칼프 사건 이후 물리적 보안 문제는 북미 전력계통 신뢰도 관리기구(NERC : NorthAmerica Federal Energy Regulation Commission)에서 주요 송전 설비 보호에 대한 새로운 표준으로 논의하기 시작하게 만들었다. 송전선로 또한 작은 공격으로 피해를 최대화 시킬 수 있는 현실적 접근 가능한 공격 대상에 속한다. 송·배전선로는 발전소와 사용자 사이에 전력을 연결하여 경제적인 전력전송이 가능하게 하는 주요 전력설비이다. 송전 변압기를 손상시킬 수 있다면 송전선로에 연계된 많은 배전선로가 전력공급에 방해 받음으로써 넓은 지역에 정전을 초래할 수 있어 'The Office of Technology Assessment'에서는 그리드에서 송전선로의 변압기는 가장 공격에 취약한 대상이라고 발표하였다. 메트칼프 변전소에 대한 총격 사건이 발생한지 불과 한 달이 지난 후에 아칸사스주 에서도 연달아 세 건의 송전선로에 대한 물리적 공격이 발생하기도 하였다.

그림 4. 메트칼프 변전소 총격 CCTV 장면

2.4 AMI 모의해킹 사례

스마트그리드 서비스를 제공하는 대부분의 구성요소들은 스마트미터와 같이 임베디드시스템으로 구성되어 있고 PLC, Zigbee, CDMA, 시리얼 통신 등과 같은 유무선 통신매체 기술들이 사용되고 있다. AMI(Advanced Metering Infrastructure) 시스템에서 NAN(Neighbor Area Network) 영역 종단에 위치한 스마트메터는 HAN(House Area Network) 영역기기 및 통신 네트워크 관리 등에 관여하고 있기 때문에 NAN 영역 기기들에 대한 보안 위협이 발생될 경우 NAN과 연결되어 있는 HAN 영역까지 보안위협이 전파될 수 있다. 또한 논리적으로 AMI시스템의 서버 영역과 마주하고 있기 때문에 모든 AMI 영역에 직접적으로 영향을 미칠 수 있다.

이러한 AMI 보안위협은 2009년부터 세계 최대 해킹 컨퍼런스인 블랙 햇(Black Hat)을 통해 매년 수편의 모의해킹 사례가 발표되고 있다. 특히 2013년 컨퍼런스에서는 스마트미터의 핵심 부품인 Maxim사의 MPU(Microprocessing Unit) 해킹 시연이 있었다. Teridian SoC(System on Chip) 솔루션 해킹을 통해 스마트미터의 펌웨어 이미지를 획득하고 획득한 이미지의 실행 가능성을 보여준 사례이다.

스마트미터의 접속인증과 암호에 사용되는 비대칭

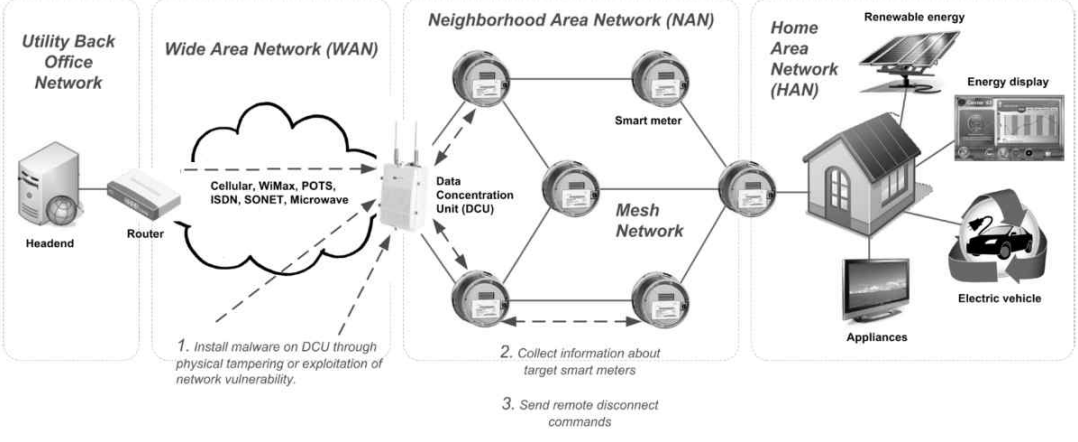
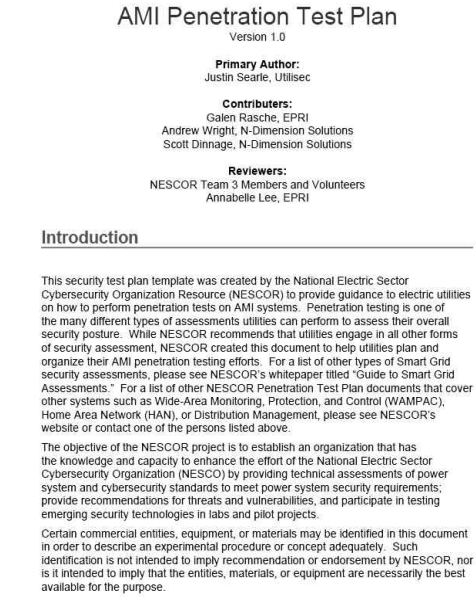


그림 5. AMI 보안 위협

그림 6. 스마트미터 MPU 해킹 시연

키에 대한 해킹시연 또한 눈여겨 볼만 하다. 스마트미터에 저장되는 비대칭키는 일반 데이터에 비해 높은 엔트로피(Entropy)를 가지기 때문에 엔트로피 분석을 통해 메모리에 저장되어 있는 비대칭키의 위치를 알 수 있는 방법이 제시되기도 하였다.



AMI Penetration Test Plan

Version 1.0

Primary Author:
Justin Searle, Utilisec

Contributers:
Galen Rasche, EPRI
Andrew Wright, N-Dimension Solutions
Scott Dinnage, N-Dimension Solutions

Reviewers:
NESCOR Team 3 Members and Volunteers
Annabelle Lee, EPRI

Introduction

This security test plan template was created by the National Electric Sector Cybersecurity Organization Resource (NESCOR) to provide guidance to electric utilities on how to perform penetration tests on AMI systems. Penetration testing is one of the many different types of assessments utilities can perform to assess their overall security posture. While NESCOR recommends that utilities engage in all other forms of security assessment, NESCOR created this document to help utilities plan and organize their AMI penetration testing efforts. For a list of other types of Smart Grid security assessments, please see NESCOR's whitepaper titled "Guide to Smart Grid Assessments." For a list of other NESCOR Penetration Test Plan documents that cover other systems such as Wide-Area Monitoring, Protection, and Control (WAMPAC), Home Area Network (HAN), or Distribution Management, please see NESCOR's website or contact one of the persons listed above.

The objective of the NESCOR project is to establish an organization that has the knowledge and capacity to enhance the effort of the National Electric Sector Cybersecurity Organization (NESCO) by providing technical assessments of power system and cybersecurity standards to meet power system security requirements; provide recommendations for threats and vulnerabilities, and participate in testing emerging security technologies in labs and pilot projects.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NESCOR, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

그림 7. AMI 취약점 방법 소개 문서

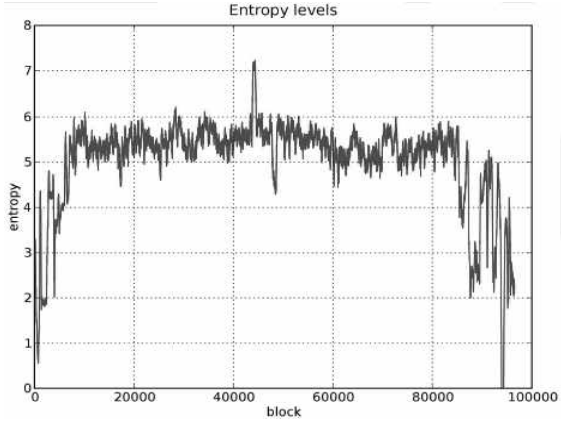
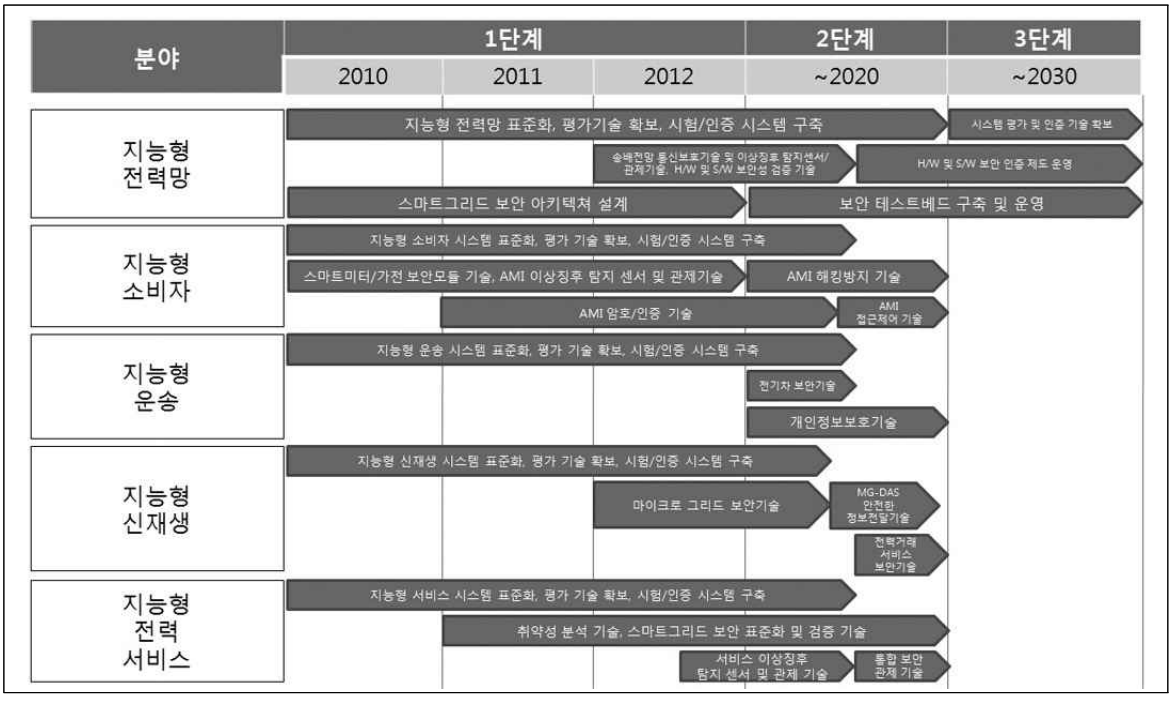


그림 8. 스마트미터 엔트로피 분석



〔그림 9〕 스마트그리드 사이버 보안 기술개발 실행 로드맵

3. 국내·외 스마트그리드 사이버 보안 기술 동향

3.1 국내 법·제도 현황

지난 2010년 1월에 발표된 스마트그리드 국가로드맵에서는 사이버 보안 분야에 대한 기술개발 실행 로드맵, 보안체계 구축 방안 내용을 담고 있다. 사이버 보안 기술개발은 스마트그리드 5대 분야 각각의 기술로드맵에 표준 및 보안 기술 분야로 포함되어 있다. 그림 9은 스마트그리드 5대분야별 보안기술 로드맵을 보여준다.

또한, TTA ICT 표준화전략맵 2012에서는 스마트그리드 표준화 전략을 마련하였다. 이 전략에서는 표준화 필요성, 시급성, 파급효과 등을 고려하여 스마트그리드 분야의 중점 표준화 항목으로 스마트그리드 보안 프레임워크, 스마트그리드에서의 개인정보보호, 스마트미터 보안 프로토콜 등이 도출되기도 하였다.

3.1.1 지능형전력망의 구축 및 이용촉진에 관한 법률 시행령

2011년 11월 25일 발효된 지능형전력망 촉진법 시행령에서는 지능형전력망 촉진법이 제정됨에 따라 지능형전력망 기본계획의 수립절차, 지능형전력망 사업자의 등록기준 및 투자비용 지원 대상, 지능형전력망 거점지구의 지정 절차 등 법률에서 위임된 사항과 그 시행에 필요한 사항을 20개 조항으로 규정하고 있다.

3.1.2 지능형전력망의 구축 및 이용촉진에 관한 법률 시행규칙

2011년 11월 25일 발효된 지능형전력망 촉진법 시행규칙에서는 지능형전력망 촉진법이 제정됨에 따라 지능형전력망 사업자의 등록, 지능형전력망 기기 및 제품 등의 인증, 인증기관의 지정 및 지능형전력망 산업진흥 지원기관의 지정절차 등 법률과 시행령에서 위임된 사항과 그 시행에 필요한 사항을 8개 조항으로 규정하고 있다. 특이사항으로는 지능형전력망 5대 기술영역에 정보보안 기술을 추가하여 정리하고 있다는 점이다.

3.1.3 지능형전력망 정보의 보호조치에 관한 지침

2012년 6월 20일 발효된 지능형전력망 지침에서는 지능형전력망 촉진법 제26조제3항에 따라 지능형전력망 정보의 신뢰성과 안전성을 확보하기 위해 지능형전력망 사업자가 준수해야 할 보호조치에 대해 42개 조항으로 규정하고 있다. 동 지침의 제2장에서는 지능형전력망 정보에 대한 기술적 보호조치를 위해 지능형전력망 시스템 보안관리, 시스템 계정관리, 비밀번호 관리, 무선통신망 보안, 정보보호시스템 운용, 악성코드 방지, 암호모듈, 암호키 관리, 지능형전력망 시스템 인증, 지능형전력망 기기 통신보안, 지능형전력망 기기 데이터보안에 대한 요구사항을 11개 조항으로 규정한다. 제3장에서는 지능형전력망 정보에 대한 물리적 보호조치를 위해 출입자 출입통제, 출입자 감시통제, 시설물 접근통제에 대한 요구사항을 3개 조항으로 규정한다. 제4장에서는 지능형전력망 정보와 지능형전력망 개인정보에 대한 관리적 보호조치를 수행하기 위해 요구사항을 규정한다. 지능형전력망 정보에 대한 관리적 보호조치를 위해서는 정보보호계획 수립, 정보보호 전담조직, 정보보호 교육 실시, 침해사고 대응체계 구축, 취약성 분석, 정보보호 시스템 정책관리, 휴대용저장매체 관리, 중요정보 보안, 보안위해물품 관리, 외부자 보안에 대한 요구사항을 규정한다. 지능형전력망 개인정보에 대한 관리적 보호조치를 위해서는 지능형전력망 개인정보 보호를

위한 일반원칙, 지능형전력망 개인정보의 수집, 고지 또는 명시, 지능형전력망 개인정보 수집의 제한, 이용 및 제공의 제한, 지능형전력망 개인정보취급자의 제한, 비밀유지, 지능형전력망 개인정보처리의 위탁, 영업의 양도 등의 통지, 영업의 양수 등의 통지방법, 지능형전력망 개인정보의 정확성 확보, 지능형전력망 개인정보의 파기 등, 동의의 철회, 열람 및 정정요구에 대한 조치, 고충처리에 대한 요구사항을 25개 조항으로 규정하고 있다.

3.2 미국 법 · 제도 현황

스마트그리드 보안분야는 2007년 에너지독립 및 안보법(Energy Independence and Security Act of 2007, EISA 2007)을 제정, 스마트그리드 운영 시 보안성을 확보할 수 있도록 법적인 지원을 하고 있다. 동법에서 사이버 보안 기술을 스마트그리드의 필수 기술로 정의하였으며, 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)로 하여금 스마트그리드 보안표준을 포함하여 스마트그리드의 상호운용성을 위한 표준을 제정하도록 하였다. 2009년 4월 미국은 중국·러시아 해커의 미국 전력망 침해사고에 대한 후속조치로서 전력인프라 보호법(Critical Electric Infrastructure Protection Act)을 발의하였고 동법에서 전력 인프라에 대한 사이버 보안 관련 긴급 명령 권한을 연방에너지규제위원회(Federal Energy Regulatory Commission, FERC)에 부여하고, 국토안보부(Department of Homeland Security, DHS)에 사이버침입에 대한 조사권한을 부여하는 등 전력망에서 발생하는 사이버 보안 및 침해사고 조사에 대한 책임 기관을 법적으로 명시하였다. 스마트그리드 관련 정책 방향 및 스마트그리드 확장에 필요한 자금 등은 관련된 미국의 복구 및 재투자법(American Recovery and Reinvestment Act of 2009, ARRA)을 제정하여 전기차, 전기 저장, 재생에너지 등과 같은 분야에서 스마트그리드 기술의 상업적 개발을 활성화하기 위한 투자에 대한 내용을 담았다. 또한, 스마트그리드 기술이 새로운 사업모델 창출, 투자대비 이윤 창출에 대한 증명이 가능하도록 실증 프로그램(Demonstration Program)에 자금을 지원하는 내용이 포함되어 있다. 다른 중요한 부분으로 스마트그리드 인력 교육 및 개발 프로그램에 대한 강화부분이 포함되어 있다. 2010년에는 국가 전력망에서 사이버 보안을 포함한 상호운용성 측면에서 발생할 수 있는 문제를 고려하여 전력망보호법(The Grid Reliability and Infrastructure Defense Act, The GRID Act)을 입법화 하였다. 이 법은 전기 분산 시스템의 신뢰성 및 인프라 보호 측면 등 전체적인 개선에 관하여 규정하고 있어 동법이 발효될 경우 사이버 보안을 포함한 스마트그리드 표준수립에 강력한 기반조성이 될 것으로 예상된다.

4. 결 론

스마트그리드 사이버 보안기술은 새로운 도전이다. 신(新)에너지시대를 이끌어갈 스마트그리드가 공격자의 악의적인 공격으로 인해 네트워크나 제어시스템이 장악된다면 사회적 혼란과 함께 금전적 피해는 상당할 것이다. 스마트그리드를 추진하는 모든 국가에서는 이러한 위험성을 인지하고 법, 제도, 연구개발 등을 통해 사이버 보안 강화에 최선의 노력을 기울이고 있다. 스마트그리드 사이버 보안전략은 이기종 지능형 전력기기의 혼재, 복합적인 네트워크 방식 그리고 대규모 스케일을 고려할 때 스마트그리드 모든 영역에서 동일한 방식의 사이버 보안기술을 적용하는 것은 현실적으로 불가능하다. 스마트그리드 영역 특성에 따라 정교한 보안대책이 필요한 것은 어쩌면 당연해 보인다. 현재의 '지능형전력망 정보의 보호조치에 관한 지침'에 따른 기술적 대책만으로 이러한 영역

특성을 반영하기에는 한계가 있어 스마트그리드 영역별로 '보안 가이드라인'이 제대로 마련되어 지지 않는다면 스마트그리드의 보안 위협에 대한 우려가 현실화 될 수 있다. 스마트그리드 기기는 대부분 임베디드 기기(Device)로 구성되어 있지만 현재 스마트그리드 서비스를 제공하는 스마트미터와 전기자동차 충전기와 같은 임베디드 기기에 대한 국내의 보안 가이드라인은 아직 마련되어 있지 않아 보안 취약성에 대한 평가도 스마트그리드 제조사가 준수해야 할 가이드가 없었다. 이미 블랙 햇을 통한 임베디드 기기에 취약성 분석 기법이 발표되고 모의침투 시연이 있었지만 아직 스마트그리드 기기에 대한 보안 위협을 대비한 충분한 준비가 되어 있다고 볼 수 없다.

지난 몇 년간 국내 지능형전력망 시범사업은 스마트그리드 개념 정립과 모델을 제시하고 관련 기술개발을 거쳐 최근 스마트그리드 사업화와 구체적인 적용사례들이 발표되고 있다. 건물 내 전력 냉난방 운영설비와 태양광·에너지저장장치(ESS)를 이용한 건물 에너지 최적화시스템과 에너지 신사업 활성화 계획의 일환으로 도서 지역의 디젤발전 시설을 태양광, 풍력 등 신재생에너지와 에너지저장장치를 결합한 친환경 에너지 자립섬을 구축하고 전국에 전기자동차 충전인프라 구축하는 등 미래 에너지 형태인 스마트그리드가 조금씩 현실화 되고 있다. 하지만 이러한 스마트그리드 사업을 착오 없이 추진하기 위해서는 스마트그리드 보안기술 없이는 불가능하다. 국내의 스마트그리드 관련 보안 로드맵과 보안 법규는 2010년 제주 스마트그리드 실증단지 구축과 함께한다. 이제 다시 스마트그리드 보안 대책에 필요한 관련 법규들과 기술개발을 위한 보안 로드맵을 정리하고 개발할 필요성은 충분하다고 생각된다.

참 고 문 헌

[1] Securing the US Electrical Grid(2014. 7)
http://www.thepresidency.org

◇ 저 자 소 개 ◇

임용훈

1996년 건국대학교 전자공학과 졸업. 1998년 건국대학교 전자공학과 졸업(석사). 1996년~현재 한전전력연구원 선임연구원.