한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Grid 공격 사례와 취약점 분석 및 보안대책

천우성°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: deux8522@gmail.com · prof1@paran.com

Vulnerability Analysis and Security Measures according to Smart Grid Attack Case

Woo-Sung Chun°, Dea-Woo Park*
°*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

Smart Grid는 전기망과 정보통신망이 융합된 형태로 발전송전배전의 전 과정에 대한 통제가 가능하고, 결과적으로 에너지 사용의 효율성을 높이고자 하는 것이 지능형 전기망이다. 정보통신망을 이용하기 때문에 기존의 다양한 사이버 보안위협으로부터 그대로 노출되어 있으며, 전기망에서의 취약점도 함께 가지고 있다. 본 논문에서는 우리나라보다 먼저 Smart Grid를 도입한 나라의 Smart Grid 공격 사례와 예상 공격에 대한 취약점을 분석하고, 분석된 취약점에 대한 Smart Grid 보안 대책을 마련한다. 본 연구를 통해 Smart Grid에 대한 보안성 강화와 사회안정성 향상에 기여하게 될 것이다.

키워드: 지능형 전기망(Smart Grid), 취약점(vulnerability), 보안대책(security measures), 공격 사례(Attack Case)

I. 서론

Smart Grid를 도입중인 미국에서 캐나다 남부지역의 대규모 정전사태가 발생하였었다. 이 사태로 주요 공항, 수도 등 기간시설이 마비되고 공장운영이 중지되는 일이 일어났다. 이에 약 6,000만 명의 해당되는 지역 주민들이 정전 피해를 입었고, 뉴욕, 클리블랜드, 디트로이트, 토론토를 포함한 북동부 주요 산업 중심지역이 피해를 입었다. 이 정전사태로 인해 미국, 캐나다 양국은 40~60억 달러에 피해가 발생한 것으로 보도되었다[1].

이와 같은 사례는 폐쇄형, 단독망으로 운영 관리하던 기존의 전기망에서 IT와 인터넷통신망이 연결되면서 인터넷 통신 네트워크에서 발생하는 보안문제가 Smart Grid 전기망에서도 나타나게 된 것이다.

특히 전기망 통제 시스템은 기존에는 공공 네트워크와 분리되어 있었으나 지능형 전기망과 연계되면서 IP(Internet Protocol) 기반 시스템이 사용되고 있다.

이와 같이 지능형 전기망에 대한 해커의 불법적인 공격으로 바이러스나 악성코드를 감염시키고 DDoS(Distributed Denial of Service)공격과 같이[2], 전기IT시스템을 무력화 시킨다면 위와 같은 정전은 물론 국가인프라인 전기 시스템에 치명적인 피해를 입힐 수 있을 것이다. 따라서 Smart Grid 보안 대책[3]에 관한 연구가 필요하다.

따라서 본 논문에서는 우리나라보다 먼저 Smart Grid를 도입한 나라의 Smart Grid 공격 사례와 예상 공격에 대한 취약점을 분석하고, 분석된 취약점에 대한 Smart Grid 보안 대책을 마련한다.

II. 관련 연구

2.1 Smart Grid

전기망에 통신망을 접목시켜 전기계통 시스템의 제어를 통하여 발전송전배전의 전 과정에 대한 통제가 가능하고, 결과적으로 에너지 사용의 효율성을 높이고자 하는 것이 지능형 전기망(Smart Grid)이다. 기존 전기망에 IT를 융합하여 전기 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 에너지 효율을 최적화하는 것이다.

그림 1. Smart Grid 구성도
Fig. 1 Smart Grid configuration

2.2 Smart Grid 구성 요소와 기술

Smart Grid 분야는 전기와 IT기술을 융합하여 다양한 서비스를 가능하게 하는 첨단 검침 인프라(AMI: Advanced Meter Infrastructure) 시스템은 물론이고, 발전, 송전 및 배전망의 전기 계통 고도화, 신재생 에너지의 활용, 전기자동차 등 에너지 및 환경 관련하여 이슈가 되고 있는 기술들 중 전기와 관련된 모든 것에 직간접적으로 관계를 맺고 있다.

고객의 프라이버시 노출, 정보 도용, 사용요금 조작은 물론, 전기시스템의 마비까지 기존 전기망에서 나타나지 않았던 새로운 위협의 가능성이 도사리고 있다. Smart Grid 전반적으로 새로운 국면의 기술적인 보안 대책이 마련되어야 하고, Smart Grid 구축과정으로부터 밀착성 있게 구현되어야 한다[4].

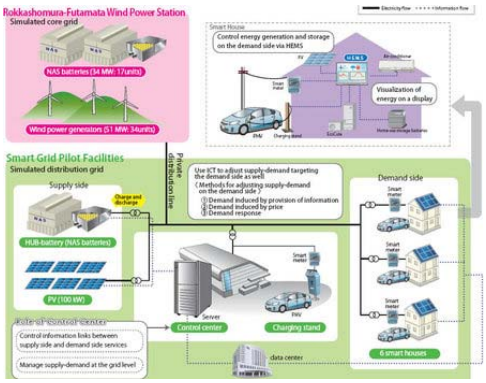

그림 2. Smart Grid 구성요소
Fig. 2 Smart Grid Component

III. Smart Grid 공격 사례 및 예상 공격

3.1 악성코드로 인한 발전소 마비

전기인프라의 보안 문제는 수년 동안 계속해서 제기되어 왔다. 시장분석기관 Gartner는 2004년에 핵심 인프라에 IP 네트워크를 사용하는 것이 사이버공격자들을 강하게 유인할 수 있다고 경고한 보고서를 낸 바 있다[5]. 2008 RSA Conference(미국정보보안기술박람회)에서 전기업체에 보안 전문가는 일반인이 흔히 사용하는 이메일 서비스를 이용하다가 악성코드(malware)를 자신의 컴퓨터에 다운로드하게 되고, 나아가 발전소 전체를 마비시키는 과정을 상세히 보여줬다. 또한, Core Security는 발전소, 석유정제소 등에서 운영 자동화용으로 사용되는 Suitelink 소프트웨어의 허점을 발견하였다[6].

3.2 Smart Grid 시스템 해킹

전기인프라 보안에 대한 경고는 현재까지 계속해서 일어나고 있다. 미국의 보안전문 회사인 IOActive는 2009년 3월에 Smart Grid 플랫폼에 커다란 보안 결함이 존재한다고 보도하였다. IOActive는 Smart Grid가 프로토콜 변경, 버퍼 오버플로우(buffer overflow), 루트킷(rootkits)과 같은 일반적인 보안 취약점들에 노출되어 있다고 주장하였다. 그리고 IOActive는 500달러의 장비와 자료, 전자기술과 소프트웨어 공학 기초 지식을 갖고 있는 사이버공격자가 디지털 계량기 인프라를 명령하고 통제할 수 있다고 주장하였다[7]. 즉, 그 정도의 사이버공격으로도 대규모의 가정 및 기업용 전기시스템이 교란 당할 수 있다는 것이다.

3.3 전기망 침투 및 교란

전기인프라의 보안 위험성에 관한 이러한 연구 및 분석은 언론에서 실제사례 보도로 이어지고 있다. 월스트리트 저널은 2009년 4월 8일 미국의 국가 전기망이 외국 해커들에 의해 침입 당했다고 보도하였다. 중국, 러시아의 해커들이 미국의 전기망 시스템에 침투해 전기망을 교란시키는데 활용되는 소프트웨어를 심어놨다고 보도하였다. 월스트리트 저널은 미국 보안당국 관계자의 말을 인용해 그 침투를 전쟁과 같은 비상시에 미국 전기망에 침투해 주요 인프라의 활성화를 차단하려는 사이버스파이의 훈련으로 추정하였다[8].

3.4 Smart Grid에 대한 예상 공격

Smart Grid의 복잡성에 따른 취약성이 나타나고, 오픈망을 통한 공격에 노출되고, 비고의적 에러를 증가시킬 수 있다. 상호 연결된 네트워크의 취약성이 있다.

통신 붕괴에 대한 취약성 및 DoS 공격이나 소프트웨어 및 시스템 무결성을 침해할 수 있는 악성 소프트웨어 공격에 노출되고, 잠재적인 공격을 위한 진입점과 경로가 증가한다. 고객의 개인정보를 포함하여 데이터 기밀성의 침해가 가능하고, Smart Grid 하부구조와 IP·기반 유선 및 무선망과의 혼합지능형 계량기, 센서, 원격 검침 및 제어 시스템 같은 새로운 네트워크 종단점의 유입·입상적(granular) 접근 정책 및 고용원, 계약자 및 소비자와 같은 원격 사용자 그룹을 위한 제어에 대한 공격이 가능하다.

IV. Smart Grid 공격에 대한 취약점 분석 및 보안 대책

4.1 Smart Grid 공격에 대한 취약점 분석

2007년 미국 에너지부의 아이다호 국립 연구소(Idaho National Laboratory)에서 전기망에 대한 사이버공격을 실험한 결과, 해커가 발전기를 통제하고 파괴할 수 있음을 여실히 보여주었다. 지능형 전기망의 핵심 기술인 첨단 검침 인프라 즉, 지능형 계량기(스마트 미터)의 취약성을 이용하면 금전적 이득을 취할 수 있기 때문에, 악성 해커의 타깃이 될 것으로 예상된다.

지능형 계량기 사이에서 확산되는 웜이 최근에 실제로 제작되었다. 계량기 봇(meter bots), 분산 서비스 거부(DDoS) 공격, 사용 기록기(usage logger), 지능형 계량기 루트킷, 계량기·기반 바이러스 및 다른 악성 소프트웨어가 출현할 것이 확실하다. 또한 지능형 전기망에 저장된 에너지 사용 정보를 통하여 고객의 비밀성이 침해되어 전기 소비 습관과 행위 등이 노출된다.

4.2 Smart Grid 보안대책

IP기반의 바이러스, 스파이웨어, 해킹과 같은 외부 공격이 전기시스템에도 그대로 위협이 될 수 있기 때문에 외부의 물리적 훼손이나 사이버 공격에 대처할 수 있는 보안 시스템이 필요하다. 보안기술로는 인증, 암호화, 가상사설망(VPN), 전자인증 등이 고려되고 있다.

Smart Grid의 보안대책을 표 1로 나타내었다.

표 1. Smart Grid의 취약성과 보안대책

Table. 1 The vulnerability of the security measures are the smart grid

취약성	항목	보안 대책
- Protocol - open Port - DB	시스템	- 시스템 감시 센서 보호 - 이종 어플리케이션 서버 및 DB 통합 보안 - 서버 및 DB 통합 보안
- 파일구조 - 악성코드 침입	H/W & S/W	- 파일 패턴탐지 보안 - H/W, S/W 보안 인증 체계 - 수요반응 프로그램 보안
- 위장 AP - 위장 Proxy Server - 스푸핑 공격	네트워크	- 차세대 통신망(IPv6) 보안 - 프로토콜 암호화 - 네트워크 접근제어 - 공격경로 역추적 및 대응/관리 - 실시간 양방향통신보안 - 실시간 통합감시 및 능동적 방어
- 패킷 암호화	무선 통신	- 송전 시스템 상태 감지 - 보안키 관리 - 통신단말 자동인증 및 관리
- 프라이버시 침해	기타	- 기관 간 보안정보 공유체계 - 네트워크 포렌식 구현

V. 결론

전기 인프라에 사이버 공격이 발생하면 국가적인 정전 사태와 같은 비상사태가 생길 것이다. 따라서 Smart Grid를 도입한 국내에서도 정부와 산업체, 학계 및 연구소 등이 컨소시엄을 형성하여 점차 지능화되고 다양화되어 있는 사이버 공격에 대응할 수 있는 보안대책을 수립하여야 할 것이다. 본 논문에서는 Smart Grid 공격 사례를 연구하고 그에 따른 취약점을 분석하여 Smart Grid의 보안대책을 연구 하였다.

지능형 전기망을 위한 정보보호 기술을 구현하기 위해서는 전체적인 보안 위험 관리 프레임워크가 개발되어야 할 것이며, 기존의 IT망의 보안 취약점과 전기망의 보안 취약점을 분석 연구하여 Smart Grid 기술에 적용되는 보안대책의 연구가 필요할 것이다.

참고문헌

[1] 구본경, “美, Smart Grid(전기IT) 프로젝트 잇따른 성공,” KOTRA, 동향자료, 2008.

[2] 천우성, 박대우, “DoS공격에 대한 N-IDS 탐지 및 패킷 분석 연구,” 한국컴퓨터정보학회 논문지, 13(6), 2008. 11.

[3] 박대우, 서정만, “TCP/IP 공격에 대한 보안 방법 연구,” 한국컴퓨터정보학회 논문지, 10(5), 2005. 11.

[4] 손소현, “Smart Grid(Smart Grid)의 현재와 추진 정책 :전기계량기의 미래 모습, Smart Grid,” 기술과미래, 60(4), 64-67쪽, 2010. 2.

[5] 이일우, 박완기, 박광로, 손승원, “Smart Grid 기술 동향,” 한국통신학회지, 26(9), 24-33쪽, 2009. 8.

[6] Mills, E., “Breaking into a power station in three easy steps,” http://sfgate-cnet.com.com, 2008. 4.

[7] 정태근, “위협받는 Smart Grid 안전 :Smart Grid 사이버테러 위협,” 정태근의원실 단행본, 2009.

[8] 전용희, “Smart Grid의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석,” 정보보호학회논문지, 20(3), 79-89쪽, 2010. 6.