한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Grid 해외 공격사례 및 한국 Smart Grid에 대한 예상 공격분석과 보안대책

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

Eexpected Attack and Security Measures for the Korea Smart Grid through

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

● 요 약 ●

2030년까지 한국에 Smart Grid를 구축할 계획을 가지고 추진하고 있다. Smart Grid는 지능형 전력망으로 기존의 전력망에 IT를 접목시켜 통신을 실시하여 양방향성을 가지게 된다. 기존의 전력망에 부가될 IT전기기기들은 기존에 IT가 지니고 있는 취약점들이 있어 기존의 Smart Grid공격에 노출되어 있다. 본 논문에서는 한국보다 먼저 구축되어서 활용되고 있는 미국의 Smart Grid에 대한 공격사례를 분석한다. 그리고 한국 Smart Grid에 대한 전기IT기기의 취약점을 분석하여, 한국 Smart Grid에 대한 예상 공격을 분석하고, 보안 대책을 제시한다. 본 논문은 한국 Smart Grid에 안정성과 보안성을 갖춘 기술 자료로 활용할 것이다.

키워드: 스마트 그리드(Smart Grid), 예상 공격(Expected Attack), 공격 사례(Hacking Attack Case), 보안 대책(Security Measures), 취약점(Vulnerabilities)

I. 서론

Smart Grid는 기존 전력망에 정보통신기술을 접목하여 전력망의 신뢰성, 효율성, 안전성을 향상시키고, 전력의 생산 및 소비 정보를 양방향 · 실시간으로 유통함으로써 에너지 효율을 최적화하는 차세대 전력망 기술이다.

기존 전력망에 IT를 융합하여 전력 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 저탄소 녹색성장이 지구적 과제로 등장하면서 온실가스 배출을 최소화하는 그린에너지 산업 혁신의 핵심으로 Smart Grid가 출현하여 에너지 효율을 최적화하는 것이다[1].

2003년 미국 북동부와 캐나다 남부지역의 8개 주에 걸쳐 대규모 정전사태가 발생하여, 공항, 수도 등 기간시설이 마비되고 공장 운영이 중지되는 일이 일어났다. 이에 약 6,000만 명의 해당 지역 주민들이 정전 피해를 입었고, 뉴욕, 클리블랜드, 디트로이트, 토론토를 포함한 북동부 주요 산업 중심지역이 큰 피해를 입었다. 이 정전사태로 인해 미국, 캐나다 양국은 40~60억 달러에 이르는 피해규모가 발생한 것으로 보도되었다[2].

이와 같이 지능형 전력망에 대한 해커의 불법적인 공격으로 바이러스나 악성코드를 감염시키고 DDoS(Distributed Denial of Service)공격과 같이, 전력IT시스템을 무력화 시킨다면 위와 같은 정전은 물론 국가인프라인 전력 시스템에 치명적인 피해를 입힐 수 있을 것이다.

특히 전력망 통제 시스템은 기존에는 공공 네트워크와 분리되어 있었으나 지능형 전력망과 연계되면서 IP(Internet Protocol) 기반 시스템이 사용되고 있다[3].

따라서 본 논문에서는 한국보다 먼저 구축되어서 활용되고 있는 미국의 Smart Grid에 대한 공격사례를 분석한다. 그리고 한국 Smart Grid에 대한 전기IT기기의 취약점을 분석하여, 한국 Smart Grid에 대한 예상 공격을 분석하고, 보안 대책을 제시한다. 본 연구의 결과를 통해 향후 구축되는 Smart Grid에 대한 사이버 보안 문제가 반드시 해결하여 우리나라가 Smart Grid 선도국가로 발전하는데 필요한 보안 기술자료를 제공하게 될 것이다.

II. 관련 연구

2.1 Smart Grid의 정의

전력망에 통신망을 접목시켜 전력계통 시스템의 제어를 통하여 발전-송전-배전의 전 과정에 대한 통제가 가능하고, 결과적으로 에너지 사용의 효율성을 높이고자 하는 것이 지능형 전력망(Smart Grid)이다. Smart Grid는 지능형 전력망이다. 뉴욕타임스의 칼럼니스트 토머스 프리드먼이 유행시킨 용어로 알려져 있으며, '현재의 전력망에 IT와 인터넷을 적용한 차세대 에너지 신기술' 혹은

'전력망에 정보기술을 접목하여 에너지 효율을 높이는 기술'정도로 설명되고 있다.

그림 1. Smart Grid의 연계도
Fig. 1. A Smart Grid in conjunction

2.2 Smart Grid 구성 요소

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

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

2.3 Smart Grid의 내용

Smart Grid는 발전 및 송배전 설비는 물론 일반 가정, 사무실, 공장 등에 설치된 각종 감시/제어 설비, 스마트 미터(smart meter), 소프트웨어, 네트워킹, 통신 인프라 등을 포함한다. 이들을 통해 전력의 생산과 공급, 소비를 최적화하고, 에너지 효율을 최대화할 수 있다. 최근 급격하게 도입이 늘어나고 있는 풍력, 태양광 발전과 같은 분산형, 신재생에너지원과 전기자동차의 운영에도 Smart Grid가 최적의 환경을 제공하게 된다. 소비자는 품질별 전력을 선택하여 공급받을 수 있고, 전력의 가격을 고려하여 소비시간을 결정할 수도 있다. Smart Grid는 전통적인 전력산업의 근간을 바꾸는 새로운 산업의 등장을 의미하는 것이다.

2.4 Smart Grid 보안 기술

기존의 전력망은 폐쇄형, 단독망 운영관리로 보안이 크게 문제되지 않았지만, IT가 결합됨에 따라 정보통신 네트워크 기기에서 발생하고 있는 보안문제가 나타날 수 있는 우려가 높다.

고객의 프라이버시 노출, 정보 도용, 사용요금 조작은 물론, 전력시스템의 마비까지 기존 전력망에서 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].

Smart Grid에 대한 외부의 물리적, 사이버 공격이 발생하여 전력망이 손실을 입을 경우 국자적인 안보 위협이 발생할 수 있으며, 스마트 어플라이언스 보안, 측정/제어 정보 무결성, 장치 간 상호인증, 크로스서비스 공격, DoS(Denial of Service)공격 방지, 제어시스템의 침해사고 탐지/대응/복구로 구성된다[5].

▶ 스마트그리드 정보보안 관리 프레임워크

다양한 규격으로 사용되고 있는 Smart Grid 정보 보안관리규격(권한관리, 접근제어, 암호화 규칙, 정보저장규칙, 정보)에 대한 표준, 보안참조모델 개발

▶ Smart Grid 제어망 보안

Smart Grid 제어망의 신뢰성 보장을 위한 인증, 접근제어, 암호화, 키 분배/관리, DDoS대응, 침입탐지/대응 구조 등에 대한 표준, DCS, PCS 시스템 보안 규격, 제어 프로토콜, 메커니즘 및 표현에 대한 표준

▶ 스마트 미터 보안 가이드라인

스마트 미터 데이터의 무결성 보장, 미터링 데이터의 보안 전송, 디바이스 상호인증 등에 대한 표준

2.5 Smart Grid의 효과

Smart Grid는 IT를 활용하여 전력생산 및 소비 정보를 양방향·실시간으로 유통함으로써 에너지 효율을 최적화하고 에너지 프로슈머(prosumer)로 에너지의 생산자(producer)인 동시에 사용자(consumer)가 될 수 있다는 의미로 정의할 수 있다. Smart Grid는 전통적인 에너지 자원과 재생 가능한 에너지 자원을 통합시키고, 에너지 소비를 감소시키기 때문에 녹색전력으로 불리며, 단기적 측면에서 Smart Grid는 온실가스 감축을 통해 환경을 개선하고, 지능적·효율적으로 기능하여 에너지자원의 비용이 상승하는 시기에 합리적이고 감당할 수 있는 가격으로 서비스를 제공할 것이고, 장기적으로는 우리 일상생활의 많은 면에서 변화를 촉진시킬 것으로 기대된다.

III. 해외의 Smart Grid 공격 사례 및 취약점 분석

3.1 미국의 Smart Grid 공격 사례 분석

전력인프라의 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[6]. 2008 RSA Conference(미국정보보안기술박람회)에서 전력업체에 보안 전문가는 일반인이 흔히 사용하는 이메일 서비스를 이용하다가 악성코드(malware)를 자신의 컴퓨터에 다운로드하게 되고, 나아가 발전소 전체를 마비시키는 과정을 상세히 보여줬다[7]. 또한, Core Security는 발전소, 석유정제소 등에서 운영 자동화용으로 사용되는 Suitelink 소프트웨어의 허점을 발견하였다[8].

그리고 보안 회사 Industrial Defender는 과거 7년 동안 전력인프라를 중심으로 100번 이상의 위협요소 평가를 한 결과 3만 4,000개의 취약점을 발견했다고 보도하였다[9].

전력인프라 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[10]. 즉, 그 정도의 사이버공격으로도 대규모의 가정 및 기업용 전력시스템이 교란 당할 수 있다는 것이다.

전력인프라의 보안 위험성에 관한 이러한 연구 및 분석은 언론에서 실제사례 보도로 이어지고 있다. 월스트리트 저널은 2009년 4월 8일 미국의 국가 전력망이 외국 해커들에 의해 침입 당했다고 보도하였다. 중국, 러시아의 해커들이 미국의 전력망 시스템에 침투해 전력망을 교란시키는데 활용되는 소프트웨어를 심어놨다고 보도하였다. 월스트리트 저널은 미국 보안당국 관계자의 말을 인용해 그 침투를 전쟁과 같은 비상시에 미국 전력망에 침투해 주요 인프라의 활성화를 차단하려는 사이버스파이의 훈련으로 추정하였다. 한편, 와이어드(Wired)는 2008년 1월 CIA가 미국 특정 지역의 여러 도시의 정전이 해커들에 의해 일어났음을 확인하였고, NSA(National Security Agency: 미국국가안전보장국)의 전 직원이자 전력 네트워크의 테러리스트 공격 시뮬레이션 전문가인 Winkler, Ira는 수년 동안 전력망에 침투해왔다고 보도하였다.

3.2 미국 Smart Grid 취약점 분석

2007년 미국 에너지부의 아이다호 국립 연구소(Idaho National Laboratory)에서 전력망에 대한 사이버공격을 실험한 결과, 해커가 발전기를 통제하고 파괴할 수 있음을 여실히 보여주었다.

지능형 전력망의 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. 만약 해커가 계량기를 침해하게 된다면, 에너지 비용을 즉각 조작할 수 있고 발전 에너지 계량기 수치를 조작할 수 있는 취약점이 존재한다.

기계적인 계량기에서 디지털 계량기로 전환됨에 따라, 공격 행위가 조잡하고 위험한 물리적 시스템 조작에서 원격 침투와 복잡하고 여러 가지 상태 정보를 보유한 컴퓨터의 조작으로 이동하게 될 것이다. 이것으로 더욱 정교한 공격이 가능하여 지고, 개인 전력 사용량에 대한 변경과 같은 소규모 공격이나, 전력망에 대한 대규모 공격 개시 형태로 전개될 수 있다. 예를 들어, 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 전력망에 저장된 에너지 사용 정보를 통하여 고객의 비밀성이 침해되어 전력 소비 습관과 행위 등이 노출된다.

Ⅳ. 한국 Smart Grid 예상 공격 분석과 보안대책

4.1 한국 Smart Grid 예상 공격 분석

- 그리드의 복잡성이 취약성을 도입할 수 있고, 잠재적인 공격 노출 및 비고의적 에러를 증가시킬 수 있다.
- 상호 연결된 네트워크가 통상적인 취약성을 도입할 수 있다.
- 통신 붕괴에 대한 취약성 및 DoS 공격이나 소프트웨어 및 시스템 무결성을 침해할 수 있는 악성 소프트웨어 유입의 가능성을 증대시킨다.
- 잠재적인 공격을 위한 진입점과 경로가 증가한다.
- 고객의 비밀성을 포함하여 데이터 기밀성의 침해가 가능하다.
- 그리드 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.

4.2 Smart Grid 취약점에 따른 보안대책

IP기반의 바이러스, 스파이웨어, 해킹과 같은 외부 공격이 전력시스템에도 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 취약점에 대한 미국과 우리나라의 대처방안을 비교해보고 그에 따른 보안대책을 표 1로 나타내었다.

표 1. 한국 스마트그리드의 공격과 취약점 및 보안대책
Table 1. Smart Grid of the attacks and vulnerabilities and security measures in Korea

항목	공격	취약점	보안 대책
네트워크	- DoS, DDoS - Spoofing - 루트킷	- 오버 플로우 - 위장 AP - 위장 Proxy Server	- 차세대 통신망(IPv6) 보안 - 공격경로 역추적 및 대응/관리 - 실시간 통합감시 및 능동적 방어 - 네트워크 접근제어 - 실시간 양방향통신 보안 - 프로토콜 암호화
무선 통신	- Sniffing - 콘텐츠 위변조 - Bugging - Jacking	- 패킷 암호화	- 송전 시스템 상태 감지 - 통신단말 자동인증 및 관리 - 보안키 관리
H/W & S/W	- 프로그램 오류 - Virus - 악성코드	- 악성코드 침입 - 파일구조	- 임베디드 시스템 보안 - 수요반응 프로그램 보안 - H/W, S/W 보안성 인증 체계
시스템	- SQL Injection - 백 도어	- Port open - DataBase - Protocol	- 시스템 감시 센서 보호 - 이종 어플리케이션 서버 및 DB 통합 보안 - 서버 및 DB 통합 보안
기타	- 보안 의식 결여	- 프라이버시 침해	- 기관 간 보안정보 공유체계 - 네트워크 포렌식 디자인 및 구현

V. 결론

전력 인프라에 2009년 7월 초에 발생한 7.7 DDoS 공격처럼 사이버 공격이 발생하면 국가적인 정전 사태와 같은 초유의 비상사태가 생길 지도 모른다.

본 논문에서는 지능형 전력망의 도입에 따른 정보보호 기술의 공격을 살펴보고 그에 따른 취약점을 분석하여 Smart Grid의 보안 강화를 강조하고, 기초 기술자료로 사용하고자 하였다.

지능형 전력망을 위한 정보보호 기술을 구현하기 위해서는 전체적인 보안 위험 관리 프레임워크가 개발되어야 한다. 기존의 IT 보안 취약점들에 대해 계속 보완작업이 이루어지고 있는데 Smart Grid 기술에도 접목시키는 작업이 필요할 것이다.

향후 연구에서는 Smart Grid만의 보완 강화 기술들에 대한 적용과 시스템에 대한 연구가 필요하다.

참고문헌

[1] 박남제, “Smart Grid 환경에서의 개인정보 취약점 분석과 보호 방안”, 한국정보기술학회논문지, 제 8권, 제 9호, 2010.

[2] 윤인하, “최근 미국 동부지역의 정전사태와 미국 전력산업의 문제점”, Asia-Pacific Review, 2003. 9.

[3] 박대우, 서정만, “TCP/IP 공격에 대한 보안 방법 연구”, 한국컴퓨터정보학회 논문지, 제10권, 제5호, 2005. 11.

[4] 이경복, 박태형, 임종인, “정보보호정책 관점에서의 한국형 Smart Grid 추진 방안에 관한 연구 - 미국과의 비교연구를 중심으로 -”, 정보화정책, 제16권, 제4호, 2009.

[5] 천우성, 박대우, “DoS공격에 대한 N-IDS 탐지 및 패킷 분석 연구”, 한국컴퓨터정보학회논문지, 제13권, 제6호, 2008. 11.

[6] 윤영직, 허준, 홍충선, 주성호, 임용훈, “전력선 통신 네트워크를 위한 혼합형 보안구조 설계”, 한국정보과학회, 2007.

[7] 피무호, 최종필, “발전소 시뮬레이션을 위한 사용자 인터페이스 설계 및 구현”, 한국정보과학회, 2005.

[8] 주재우, “미·일·중·러의 대외에너지 안보전략과 에너지 협력 가능성 진단”, 동북아에너지협력연구, 2003.

[9] 이건희, 서정택, 이철원, “스마트그리드 사이버 보안 추진 현황”, 제 20권 제 5호, 2010.

[10] 이승재, 최면송, “차세대 전력시스템 보호제어 기술의 연구동향”, 제 50권 제 11호, 2001.