한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

BlackList의 Smart Grid 취약점 및 보안 적용 방법 연구

이보만°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: bomans@nate.com, prof1@paran.com

A Study of Applying BlackList for Smart Grid Vulnerability and Security

Bo-Man Lee°, Dea-Woo Park*
°*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

지능형 전력망인 Smart Grid의 등장으로 미국, 일본 등의 국가는 Smart Grid 시장을 선점하기 위해 노력하고 있다. 한국 또한 경쟁국으로서 G20 정상회의에서 Smart Grid 시범 단지를 선보이려고 준비 중에 있다. Smart Grid의 발전에 기본적인 전력기기와 IT기기의 융합 모델인 전력IT기기의 연구가 진행되고 있고, 단일 전력 기기일 때 와는 달리 IT 기기의 특성에 따른 보안 문제에 노출되어 보안에 대한 연구가 필수적이다. 본 논문에서는 Smart Grid에 사용되는 전력 IT 기기에 적용 할 수 있는 보안 방법인 BlackList 설정을 연구하여 Smart Grid 시대의 발전에 기여 할 것이다.

키워드: 지능형 전력망(Smart Grid), 취약점(vulnerability), 보안(security), 블랙 리스트(BlackList)

I. 서론

Smart Grid[1]는 전력망에 IT 통신 인프라를 연동한 차세대 전력망의 모델이다. 제주도에서 2010년 11월 열릴 G20 정상회의에서도 'Smart Grid 주간'을 지정하여 Smart Grid 시범단지를 완성하여 우리나라의 기술력을 세계에 선보이고 Smart Grid의 기술표준을 우리가 주도하려고 한다.

Smart Grid의 가장 큰 특징 중 하나는 전력의 생산자와 사용자 간에 양방향 통신이 가능하다는 것이다. 실시간 전력가격 등의 정보가 사용자에게 전달되어 사용자가 전력소비의 시간을 결정할 수 있고, 사용자의 부하상황 등 다양한 정보가 계통의 운영자나 전력의 생산자에게 전달됨으로써 전력 생산의 조절과 계획도 가능하다. Smart meter는 전력의 사용을 시간별로 기록하고 통신함으로써, 전력수요가 많고 적음에 따라 전력가격을 다르게 부과하는 것이 가능하도록 한다. 이러한 시간대 별 차등 요금제도는 일종의 경제적 인센티브로서 전력사용을 수요가 집중되는 시점으로부터 분산시키는 효과를 거둘 수 있다. 그러나 양방향 통신의 역기능으로 사용자가 공격자가 될 수 있게 되었다.

한국이 이미 구축해본 네트워크 통신 기술을 이용하면, 타 국가와의 주도권 싸움에서 유리하다. 하지만 우리나라가 Smart Grid 기술을 선도하기 위해서는, 보안 역시 빼놓을 수 없는 문제이다. Barack Obama 미국 대통령도 새 백악관 사이버보안 담당자를 선발하기 위한 조건 중 하나로 Smart Grid 보안을 꼽았다.

본 논문에서는 Smart Grid의 전력망이 취약점이 발견되어 공격을 당해 피해를 입는 것에 대비하여, 공격에 대한 모든 정보를 포함 할 수 있는 Smart Grid 보안 Black List 설정을 연구하고, 전력 IT 기기에 적용 할 수 있게 함으로서 Smart Grid 시대의 발전에 기여 할 것이다.

II. 관련 연구

2.1 Smart Grid의 정의

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 등 전력과 IT 관련 기술[2],[3]과 인프라를 모두 포함한다. 이들을 통해 전력의 생산과 공급, 소비를 최적화하고, 에너지 효율을 최대화할 수 있다. 최근 급격하게 도입이 늘어나고 있는 풍력, 태양광[4] 발전과 같은 분산형, 신재생에너지원과 전기자동차의 운영에도 Smart Grid가 최적의 환경을 제공하게 된다[5]. 사용자는 품질별 전력을 선택하여 공급받을 수 있고, 전력의 가격을 고려하여 소비시간을 결정할 수도 있다. Smart Grid는 기존의 전력산업을 대체하는 새로운 시대의 등장을 의미한다.

그림 1. 스마트그리드 구성도
Fig. 1 Smart Grid configuration

III. Smart Grid 취약점 및 보안 연구

3.1 Smart Grid가 가지는 취약점

Smart Grid에서 취약점을 IT전력기기 관점에서 볼 때, 다음과 같은 4분야 등으로 나누어서 취약점을 분석한다.

1) 스마트 제어

사용자의 스마트 제어 영역에서는 '인증(authentication)', '사용자 데이터 수집(collection of consumer data)', '상호운영성(interoperability)', '전력 사용에 대한 통제권(control overpower usage)'의 보안 취약점이 존재한다.

2) AMI(스마트 미터기)

스마트 미터기와 관련된 보안 취약점에는 '스마트 미터기에서의 프라이버시(privacy in smart meter)', '스마트 미터기에 대한 접근통제(access control of smart meter)'에 대한 보안 취약점이 존재한다.

3) 기반 통신

Smart Grid의 기반 통신망 영역의 보안 취약점에는 '유 · 무선 통신 네트워크에서의 취약점(vulnerability of wire/wireless communication network)'과 '전력선 기반 통신에서의 셀 보안 취약점(security vulnerability of cell in power line-based communication network)'이 존재한다.

4) 서비스 제공자

서비스 제공 사업자 영역에서의 Smart Grid 보안 취약점에는 '사용자 데이터의 소유권(ownership of comsumer data)', '사용자 데이터의 프라이버시(privacy in comsumer data)', '사용자의 전력사용에 대한 통제(control over power usage)'와 같은 취약점이 존재한다.

3.2 Smart Grid 보안 방법

취약점에 대한 보안을 하기 위해서는 정보보호[6]의 기본요소인 기밀성,무결성, 가용성, 인증, 부인방지, 접근제어를 통해 보안을 한다.

1) 기밀성 보장

기밀성 보장을 위한 대표적인 보안 방법은 데이터 암호화이다. 암호화는 비밀키(security key)를 이용하여 원본 데이터를 특정 알고리즘에 따라 변형시킴으로써 비밀키를 가지고 있는 사람만이 암호를 풀어서 원본 데이터를 읽을 수 있도록 하는 방법이다.

스마트 제어 영역에서 사용자 데이터 수집 이라는 취약점을 방어 하려면, 사용자 데이터를 암호화하여 기밀성을 보장해 줌으로서 해결을 할 수 있다. AMI 부분에서도 스마트 미터기에 저장된 개인정보를 암호화함으로서 스마트 미터기에서의 프라이버시 문제를 해결 할 수 있다.

2) 무결성 보장

Smart Grid의 기반 통신망 영역의 무결성 보장을 위해서는 수신자가 데이터가 중간에 변형이 되었는지 여부를 확인할 수 있어야 한다.

기반 통신에서 유 · 무선 통신 네트워크에서의 취약점을 방어하려면, 메시지를 변형이 되었는지의 여부를 알 수 있는 메시지의 인증코드 값을 생성하게 된다. 메시지인증코드 알고리즘은 송신자와 수신자가 미리 공유하는 세션키(session key)라고 불리는 비밀키와 암호화HMAC(keyed-Hash Message Authentication Code) 알고리즘을 이용한다.

3) 가용성 보장

가용성 보장은 Smart Grid기기가 정상적으로 작동하지 못하도록 서비스거부 공격을 방지하는 것을 말한다. 서비스거부 공격이란 전력IT기기가 작동 할 때 사용되는 CPU, 통신 대역폭 등의 시스템 자원을 의도적으로 소모시켜 해당 시스템을 마비시키거나 정상적인 동작이 불가능하도록 만드는 공격을 말한다. 대표적인 예로 유명한 DoS[7]나 DDoS 공격이 있다.

스마트 제어 부분에서 서비스 거부 공격인 DDoS 공격을 받게 되면 전력망 내의 중요 시스템이 제어가 불가능한 상황이 되어 정상적인 동작을 못하게 되거나 관리자[8]가 시스템에 접속할 수 없게 되어 치명적인 결과를 초래할 수 있다.

4) 부인 방지

부인방지는 Smart Grid기기가 전력의 공급과 차단 및 과전류 등의 작동을 할 때 사용되는 정보를 데이터의 송수신자가 자신의 데이터 송수신 사실을 부인할 수 없도록 하는 것을 말한다.

기반통신에서는 부인방지를 위하여 통신 메시지에 암호화된 고유한 값을 같이 보내주는 인증서를 사용하게 되는데, 서비스 제공자의 사용자 데이터의 소유권 문제에서도 전력망에서 다른 사업자 간이나 고객 간에 통신을 할 때 송수신자 한쪽이 자신의 이익을 위해 송수신 사실을 부인하는 경우가 있을 수 있다.

이때에도 사용자가 보낸 데이터를 소유권자의 인증서를 저장함으로서 차후 사용자가 데이터를 보낸 사실이 없다고 하는 것을 방지 할 수 있다. 수신 부인방지를 위해서는 인증서 사용과 함께 네트워크 감시를 실시하여야 한다. 네트워크 감시를 통해 네트워크 상의 데이터 흐름을 기록해 두면 추후에 있을 송수신 부인을 방지할 수 있다.

5) 인증(authorization)

인증은 Smart Grid기기가 통신 네트워크상의 사용자나 장치들에 대한 접근과 제어를 할 때, 접근자는 고유의 신분증을 사용하여 서로가 누구인지, 신뢰할만한 대상인지를 판단하도록 하는 일종의 확인 과정이다. 기반통신에서 대상이 누구인지 확인하는 방법으로 인증이 사용되는데, 스마트 제어 부분에서도 인증을 사용하여 정당한 사용자와 그렇지 않은 사용자를 구분할 수 있도록 할 수 있다.

6) 접근제어(Access Control)

접근제어는 시스템에 접근 권한을 차등적으로 부여하는 방법이다. 예를 들어 배전소 관리 시스템의 경우 최종 관리자는 모든 관리 권한을 부여 받지만, 송전만을 관리하는 관리자의 경우 송전에 관련된 권한만 부여받는다. 접근제어를 위해서는 이미 인증된 대상에 적절한 권한부여(authorization)가 필요하다. 기반통신에서는 접근 제어를 위해 사용자별 권한부여 DB를 사용하게 된다.

스마트 제어 부분에서 전력 사용에 대한 통제권 보장을 위해 권한부여 DB를 사용하여 비정상적 전력 사용을 방지하고, 스마트미터기의 경우에는 스마트 미터기에 대한 접근통제를 위해 권한부여 DB를 사용하여 전력량을 조작하는 상황이 발생하지 않도록 한다. 서비스 제공자 분야에서는 권한부여 DB를 사용하여 허가되지 않은 곳에 전력을 전송하는 일이 없도록 할 수 있다.

IV. Smart Grid 보안을 위한 BlackList 적용방법 연구

4.1 BlackList 내용 생성

Smart Grid 보안을 위한 BlackList 내용으로는 취약점 종류, 관련된 전력망, 공격 시작지, 공격대상지, 공격 경유지, 공격의 강도, 공격 전파 속도, 공격에 사용되는 프로그램 및 도구, 공격의 특징, 유사한 공격의 종류, 방어 시작지, 방어 소요 시간, 방어 방법 등이 포함된다.

전력 IT기기 들도 실시간으로 위협을 탐지하고 자동적으로 대처 할 수 있게 하기 위해, 평상시 전력망들의 특성인 평균 전력 사용량, 허가 가 가능한 전력 초과 사용량, 전력 사용지의 정보, 평균 통신 회수 등이 포함되어 미 탐지된 공격 또는 예외 사항을 처리 할 수 있도록 구성한다. 구성된 BlackList는 가정용, 상업용, 기업용, 농수산업 등의 생산용, 발전용 등의 전력망의 특색에 맞게 전력 IT 기기에 적용 가능하게 구성하고, 전력 IT 기기가 전달받은 BlackList를 적용할 수 있도록 생성한다.

4.2 BlackList 적용 방법

BlackList를 적용하는 방법에는 하드웨어적인 방법과 소프트웨어적인 방법이 있다. 하드웨어적인 방법으로는 전력기기에 별도의 BlackList 방화벽을 장착 또는 연결하는 방법이 있으며, 소프트웨어적인 방법으로는 장비에 프로그램을 설치하여 논리적으로 BlackList를 설정하여 방어하는 방법이 있다.

Smart Grid에 사용되는 전력 IT 기기들은 IT 기술이 융합된 기기들인 만큼, 두 가지 방법이 모두 가능하며, 작성한 BlackList 또한 두가지 방법 모두에 적용 할 수 있다. 따라서 기기의 중요도에 따라 사용자 측인 스마트 미터기 쪽에서는 저가인 소프트웨어를 사용하고, 관리자 측인 Smart Grid 관리 시스템에서는 하드웨어적으로 고가이면서 기능 면에서 뛰어난 BlackList 기반의 방화벽을 설치하는 방법으로 설정해야 할 것이다.

4.3 BlackList의 활용

Smart Grid 보안을 위한 BlackList가 이용이 가능한 곳을 살펴보면, 먼저 Router에서 BlackList를 적용하면 IT통신의 중간에서 돌아다니는 패킷을 처리하는 곳에서 보안을 적용하는 것이기 때문에 악의적인 공격을 중간에서 차단 할 수 있다. 또한 접근제어 시스템에 적용하면 불법 사용자 색출이 가능하며, Firewall이나 IPS(침입차단시스템) 에서도 설정하여 이용하면 악의적인 공격을 탐지할 수 있어 Smart Grid의 보안성을 항상 시킬 수 있다.

V. 결론

본 논문에서는 차세대 전력망인 Smart Grid의 전력소비의 합리화, 효율성, 사용자 중심의 서비스, 녹색 에너지 사용의 극대화 등의 장점을 인식하였다.

또한 기존 전력망 에서 Smart Grid 시대로 가기위한 IT 기술과의 융합을 통한 역기능에 주목하여 해킹 등의 공격에 무방비 상태로 Smart Grid가 노출 될 경우 전력망이 마비되는 등의 금전적, 국가적 손실을 입는 것을 방지하고자 Smart Grid 취약점 및 보안 방법을 분석하고 Smart Grid 보안을 위한 BlackList를 생성 하고 적용 시키는 방법의 연구를 통해 Smart Grid 시대의 발전에 기여하였다.

향후 연구로는 Smart Grid 보안 BlackList의 하드웨어적인 적용과 소프트웨어적인 적용에 따른 차이점과 그 보완법을 분석하는 등의 연구가 진행되어야 할 것이다.

참고문헌

[1] 이일우, 이정인, “스마트그리드 정보통신기술,” 정보와 통신 : 한국통신학회지, 27(11), 3-11쪽, 2010. 11.

[2] 정영곤, 최현우, 염홍열, “스마트 그리드 보안 동향,” 정보보호학회논문지, 20(4), 66-79쪽, 2010. 8.

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

[4] 이명훈, 정범진, 김창섭, 손성용, “한국형 스마트 그리드 정보보호 표준 방향 연구,” CICS 정보 및 제어 학술대회 논문집, 2009.

[5] 이종민, 장우혁, 정방철, “스마트 그리드 전기자동차를 위한 자기장 통신 시스템 구현 연구,” 한국통신학회논문지, 35(9), 1381-1389쪽, 2010. 9.

[6] 임송빈, 오영환, “스마트 그리드 네트워크에서 효과적인 Zigbee 인증 프로토콜에 관한 연구,” 한국통신학회논문지, 36(2),

184-194쪽
[7] 이일우, 박완기, 박광로, 손승원, “스마트 그리드 기술 동향,” 한국통신학회지 (정보와통신), 26(9), 24-33쪽, 2009. 8.
[8] 정영곤, 최현우, 염흥열, “스마트 그리드 보안 동향,” 정보보호학회지, 20(4), 66-79쪽, 2010. 8.