Smart Phone을 통한 Smart Grid 네트워크 접속에서 취약성

이재현* · 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

Analysis of Smart Grid Network Vulnerability Using Smart Phone

Jae-Hyun Lee* · Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

E-mail : *Leejh9708@paran.com □ *prof1@paran.com

요 약

Smart Phone 보급이 확산되면서 인터넷 PC를 대체하는 모바일 통신으로 활용되고 있다. Smart Phone은 기존의 전력망과 IT가 융합된 Smart Grid에도서 업무용으로 사용되고 있다. 따라서 Smart Phone을 통한 Smart Grid 네트워크 접속에서 접속과 제어에 대한 보안 취약점과 Smart Grid 네트워크에 대한 취약점에 대한 연구가 필요하다. 본 논문에서는 Smart Phone을 사용하여 Smart Grid 네트워크를 통한 전력망 시스템에 접근할 때의 접속 취약점에 대한 연구를 한다. 또한 Smart Phone을 사용하여 Smart Grid 네트워크에 접속 한 후에 전력정보, 통제정보, 개인정보 등에 대한 접근 권한을 탈취 가능성에 취약성을 분석하여 발생하는 문제점과 대해 연구한다. 그리고 Smart Phone을 통한 Smart Grid 네트워크 보안 취약점에 대한 보안 강화를 위한 연구 방향을 제시하고자 한다.

ABSTRACT

Smart Phone supplies are diffused and substitute the Internet PC with Mobile communications which they are applied. Smart Phone in Smart Grid where electric power watch and the IT of existing amalgamate are used with business. Consequently from Smart Grid network connections which lead Smart Phone in about connection and control in about security vulnerabilities and Smart Grid networks the research is necessary in about vulnerability. It uses Smart Phone from the present paper and when approaching electric power watch systems which lead Smart Grid networks, it researches in about connection vulnerability. Also it uses Smart Phone and after connecting in Smart Grid networks a vulnerability in seizure possibility and, electric power information and control information, about private data etc. access authority it analyzes with the problem point which occurs it confronts it researches. And the research direction for a security reinforcement under presenting boil in about Smart Grid network security vulnerabilities which lead Smart Phone.

키워드

Smart Phone, Smart Grid, Security, Network Vulnerability

Ⅰ. 서 론

Smart Grid에서 핵심적 역할을 담당하는 것이 Smart Phone이다. Smart Phone은 모바일 결제, DMB, GPS 등 WiFi, 3G를 이용한 무선인터넷을 제공한다. 기존의 전력망에 IT가 융합된 형태의 Smart Grid는 Smart Phone을 이용해 실시간으로 전기사용량을 외부에서 확인할 수 있고 또한 전기기기의 동작을 컨트롤함 으로써 에너지 사용의 효율성도 증대시킬 수 있다[1].

Smart Grid는 인터넷의 취약성으로 무선 네트워크, 무선 주파수 등 외부의 공격 위협에 노출될 수 있다. 해커가 이러한 취약성을 이용해 공격한다면 전력정보유출, 개인정보유출 등 피해가 있다. 특히, 전력기기의 전력사용량을 통제하는 중앙관제 시스템에 대한 공격은 대정전 사태로 직결될 수 있다. 따라서 Smart Phone을 이용한 Smart Grid 환경에서의 보안이 필요하다[2][3].

실제 최근 전력망에 대한 공격 위협이 증가하고 있고 실제 공격 사례도 지속적으로 보고되는 등 Smart Grid에 대한 보안에 대한 대책이 시급한 실정이다. 이에 본 논문에서는 Smart Phone을 이용한 Smart Grid에 환경에서의 보안성 강화를 위해 수행해야 할 보안 방안을 제시한다.

Ⅱ. 관련연구

2.1. Smart Phone의 개념

Smart Phone은 기존의 휴대전화에 고기능 범용 OS를 내장되어 있고 WiFi망과 3G망을 통해 인터넷 통신을 통해 언제 어디서나 정보의 접근이 가능하다. 또한 다양한 어플리케이션 설치를 통해 사용자가 원하는 프로그램을 설치와 삭제가 가능하다.

그림 1과 같이 전 세계 Smart Phone 판매량은 2010년 28,550만대이며, 2013년에는 50,770만대에 이를 전망이다.

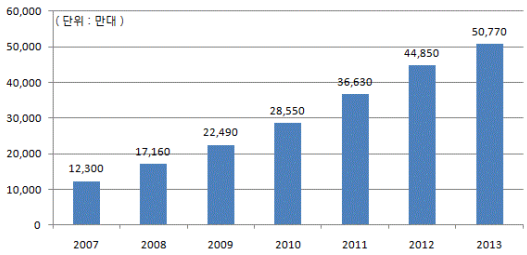

그림 1. 전세계 Smart Phone 판매 추이

2.2. Smart Grid 개념

스마트 그리드는 그림 2와 같이 전기자동차 배터리, 녹색에너지, 국가안보 송전망이용 등 효율적인 에너지 소비 방식으로 운영되는 전력시스템이다.

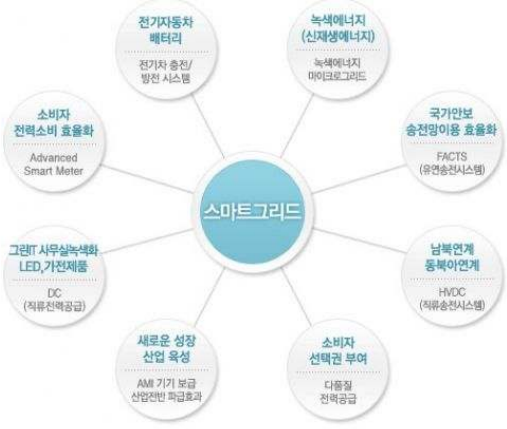

그림 2. Smart Grid

또한 Smart Grid는 소비자와 공급자의 상호작용이 가능하고 사고에 대한 자가 복구 기능을 갖추고 있어 에너지 시장의 수요에 대응할 수 있다 [4][5].

Ⅲ. 취약성 분석

3.1. Smart Phone 취약성 분석

시간과 공간에 제약 없이 무선인터넷이 가능한 Smart Phone이 확산되면서 기존 PC에서의 인터넷 환경도 Smart Phone에 환경에 맡게 변화되고 있고 이러한 변화에 대응할 수 있는 보안기술도 등장하고 있다. 하지만 PC 환경에서 사용되고 있는 방화벽, 백신이 Smart Phone 환경에서의 적용이 보편화되어 있지 않아 악성코드감염에 노출되어 있다.

Smart Phone 악성코드는 성장과 더불어 규모면에서 빠르게 증가하고 있고, 위협요인도 다양화되고 있다. 무선인터넷 사용 시 웹페이지에 암호화가 되어 있지 않고 악성코드가 삽입되어 있다면 이는 Smart Phone뿐만 아니라 PC까지 악성코드에 감염될 가능성이 있다.

Smart Phone 어플리케이션의 악성코드는 악의적인 목적을 가진 개발자의 의해 제작 및 유통되고 있으며 단말기 장애, 금전적 피해, 배터리 소모, 개인정보 유출 등의 피해를 유발할 수 있다.

그림 3은 Smart Phone 악성코드인 테러리스트 다이얼이 감염된 화면이다. 이는 Smart Phone 악성코드로 Window Mobile 환경에서 발견되었다. 모바일 게임에 악성코드는 은닉하여 유포한 것으로 카페, 공유 사이트 등으로 전파되었다. 테러리스트 다이얼은 트로이목마 형태로 작동되며 자동으로 해외 Premium-rate number에 국제전화를 시도하여 과금을 부과시키는 과금형 악성코드이다.

그림 3. 테러리스트 다이얼 감염

이러한 어플리케이션 악성코드는 3G, WiFi와 같은 무선통신환경과 PC를 이용한 유선방식으로 어플리케이션을 이동시켜 감염되기도 한다.

Smart Phone 악성코드는 초기에 단순히 단말의 기능적 동작을 마비시키는 형태에서 단말기 안에 저장되어 있는 개인정보의 유출 및 금전적 이득을 목적으로 변화되고 있다.

악의적 목적의 개발자나 해커는 악성코드나 삽입되어 있는 프로그램 즉 해킹 툴을 제작하여 스마트그리드 전력망에 침입하여 통제권을 빼앗아 개인정보를 탈취하거나 전력정보를 조정하여 해

당 건물을 정전시키는 등 피해가 가능하다.

그림 4는 Smart Phone을 이용해 전력망의 전력정보를 확인을 나타낸다.

그림 4. Smart Phone을 이용한 전력망 확인

3.2. Smart Grid 취약성 분석

Smart Grid에는 스마트계량기, 유□무선 네트워크, 소프트웨어 등 다양한 기술들로 구성되어 있다. 따라서 이에 대한 보안 문제가 발생 할 수 있다. 그림 5는 Smart Grid 취약점을 나타낸다 [6][7].

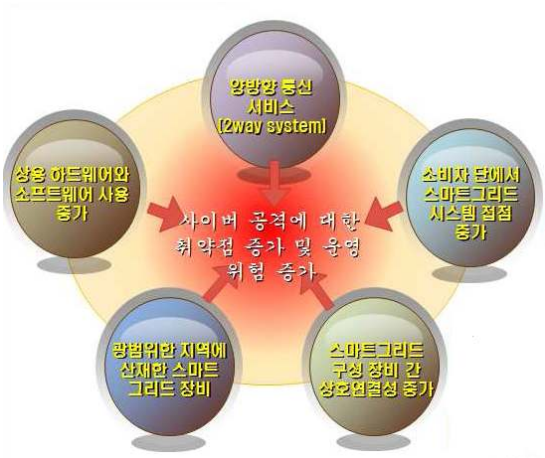

그림 5. Smart Grid 취약점

3.2.1 계량기의 램 공격

보안전문가 트래비스 굿스피드는 해커들이 직접적으로 스마트 계량기 램을 공격하고 쉽게 계량기를 통제할 수 있다고 경고한다. 만약 계량기가 보안기능을 제대로 갖추지 못하고 있다면, 해커들은 주사기를 이용해 계량기의 메모리칩의 각 측면에 바늘을 삽입할 수 있다. 그 바늘은 메모리칩의 전기 신호를 가로채는 정찰병 역할을 한다. 그 신호를 분석함으로써, 해커들은 계량기의 프로그래밍을 조정할 수 있다. 계량기가 어느 정도의 보안기능을 가지고 있다고 해도, 별도의 도구를 이용해 정보를 빼낼 수 있을 것으로 보인다.

3.2.2 계량기의 디지털 주파수 크래킹

트래비스 굿스피드는 램해킹과 유사한 기술이 스마트 계량기의 무선 주파수를 조정할 수 있다고 한다. 이런 방식을 통해 전력망 자체를 공격할 수 있다. 스마트 계량기의 양방향 무선 칩은 계량기가 원격으로 정보를 읽고, 네트워크상의 명령을 받아들일 수 있는 기능을 갖고 있다. 그 침의 소프트웨어는 보안코드를 갖고 있는데, 계량기의 프로그래밍을 크래킹 한 해커가 네트워크에 침투하기 위해 그 보안코드를 활성화 할 수 있다.

3.2.3 계량기를 무선으로 크래킹

보안전문업체 IOActive의 데이비드 베어커는 해커들이 네트워크상에서 상호 통신하는 계량기의 무선 네트워크 장치를 이용해 계량기에 침투할 수 있다고 경고한다. 공격자들은 SDR(Software Defined Radio)을 이용해 네트워크의 무선 통신을 해킹할 수 있고, 시간에 따라 계량기와 통신하는 방식을 변화시킬 수 있다. SDR이란 하드웨어 즉 단말기나 칩을 바꾸지 않고 소프트웨어 조작만으로도 셀룰러, PCS, WiBro, 무선랜, 위성통신과 같은 다양한 무선 통신 서비스를 하나의 단말기에서 이용할 수 있게 하는 기술이다.

3.2.4 네트워크에 악성코드 확산

해커가 스마트 계량기의 프로그래밍에 접속했다면, 그는 쉽게 네트워크 자체, 스마트 계량기, 전력망에 부착된 다른 장치를 공격하는 웜(Worm)이나 다른 악성코드에 노출될 수 있다. 스마트 계량기를 통해 자가 전파하는 웜을 시뮬레이션 한 결과, 24시간 내 1만5천 가구가 그 웜에 감염됐다.

Ⅳ. 보안 방안

4.1. Smart Phone 보안 방안

PC환경에서의 인터넷을 Smart Phone에서도 이용되면서 편리함과 동시에 해킹의 문제를 함께 포함하고 있다. Smart Phone의 무선인터넷 환경 역시 IP기반으로 운영되고 있어 PC에서 접근경로를 이용한 해킹공격이 Smart Phone에 발생할 수 있다. 따라서 Smart Phone 기기에 대한 공인인증이 활성화되어 보안에 대한 신뢰성과 안정성을 확보하는 것이 중요하다. Smart Phone 공인인증은 인증기관을 통해 인증서를 발급받고 인증을 한다.

앱스토어에서는 등록된 애플리케이션의 심의

및 안전성 검증을 수동으로 진행하거나 보안을 위한 검증 절차가 이뤄지지 않고 있어 애플리케이션에 악성코드가 존재하는지 확인하는데 한계가 있다. 따라서 애플리케이션의 안전성을 확보하기 위해서는 애플리케이션의 유통□인증 기술과 앱스토어에 등록된 애플리케이션에 대한 보안 검증 기술이 필요하다.

개발자는 자신이 개발한 애플리케이션의 공인인증서를 통한 신원증명을 하고 보안성 검증 센터에서 안전성 여부를 확인하는 절차를 거침으로서 이상 유무를 확인한다.

또한 주요 정보가 포함된 Smart Phone의 분실을 방지하기 위해 해당 파일의 암호화를 통해 분실하더라도 주요 내용을 제 3자가 확인할 수 없도록 해야 한다.

4.2. Smart Grid 네트워크 보안 방안

Smart Grid 대한 보안 방법은 다음과 같다.

Smart Grid 구축 및 운영에서 사이버 보안 안전성과 상호 운영성을 확보하기 위해 Smart Grid 보안 요구사항을 도출 및 보안체계 수립이 필요하다. 또한 보안기술에 대한 표준화 및 검증도 수행하여야 한다.

Smart Grid에 도입되는 하드웨어, 소프트웨어의 대한 보안성을 사전에 검증하는 보안성 검증기관을 설립하여 구축□운영시의 취약성을 분석하여 제거한다.

암호□인증을 통한 Smart Phone을 이용한 Smart Grid 접속을 통한 침해사고 예방하기 위해 인증기관에서 인증서를 발급하여 네트워크간의 상호인증을 통해 침해 전이를 방지하여 데이터 보호를 한다.

보안 등급별 접근요소의 차별화를 하여 Smart Grid의 주요 기기인 스마트 계량기에 Smart Phone을 이용한 비인가 접근 시 접근제어 및 로그관리로 취약성에 대응한다.

표 1. Smart Grid 네트워크 보안 방안

분류	보안 방안
물리적 보안	옥외에 위치된 스마트 계량기의 보호, 1차원적 잠금장치, 전자기 펄스(EMP) 공격 대비, 조작가능 성 및 경보 기능 등 물리적인 위협에 대한 대비를 요구하고 있다.
네트워크 보안	네트워크적 보안요소로는 다양한 무선 표준 활용에 대한 보호 기준이 필요하며, 송·변전 감시(SCADA)나 배전(DAS) 등에서 명확한 네트워크 분리와 인증부분에서 보안 등급별 접근요소의 차별화가 필요하다.
암호화 보안	무선센서에서 암호화를 사용할 수 있도록 하는 경량 암호 및 센서 보안 네트워크를 개발하여야 한다.

V. 결 론

Smart Phone과 Smart Grid의 공통점은 기존의 일방적인 서비스 방식에서 소비자와 개발자나 또는 정보제공자의 교류가 실시간으로 전달된다는 것이다. 즉 소비자 스스로 선택하고 확인하여 결정할 수 있는 권한이 생김으로서 국가적 해결문제가 아닌 개인의 문제는 보안지침을 확인하여 개인정보를 보호해야 한다는 것이다.

Smart Phone 서비스 환경을 보장하고 향후 발생 가능한 모바일 보안 위협에 대해 사전 방어체계를 구축하기 위해서는 Smart Phone 보안기술과 더불어 원격 보안 관리, 안전한 결제 서비스 지원 및 앱스토어를 통해 배포되는 애플리케이션에 대한 검증이 필요하다. 따라서 애플리케이션의 보안성 검증단계를 거쳐 안정적인 어플리케이션의 설치할 수 있도록 해야 한다.

Smart Grid에 대한 보안으로는 Smart Grid에 탑재될 기기에 대해서는 검증기관에 사전 검증을 통해 소프트웨어, 하드웨어에 대한 안정성과 신뢰성을 확보해야 한다. 또한 Smart Grid 접근 시 인증을 통해 비인가에 대한 접근을 제어 강화하여 불법적인 행위로 접근하려는 해커에 대한 사전 방어가 필요하다.

향후 연구에서는 Smart Phone을 이용하여 Smart Grid 공격을 하였을 때 실시간으로 공격기법 분석과 역추적을 통한 포렌식 방법론을 통해 증거자료를 확보하는 연구에 기여할 것이다.

참고문헌

[1] 이경복, 독고지은, 유지연, 이숙연, 임종인, “스마트 그리드에서의 소비자 참여와 보안 이슈”, 정보보호학회, 제 19권 제 4호, pp.21-35, 2009. 8.

[2] 이건희, 서정택, 이철원, “스마트그리드와 사이버 보안”, 한국통신학회, 제 27권 제 4호, pp.23-30, 2010. 3.

[3] 전용희, “스마트 그리드의 취약성, 특성, 설계원칙 및 보안 유구사항 분석”, 한국정보보호학회, 제 20권 제 3호, pp.79-89, 2010. 6.

[4] 박남제, 안길준, “스마트 그리드에서의 프라이버시 보호”, 한국정보보호학회, 제 20권 제 3호, pp.62-78, 2010. 6.

[5] 이정훈, 박대우, “스마트 그리드 기술에 대한 해킹과 보안 연구”, 대한전기학회 2010년 하계학술대회, pp.149-156, 2010. 7.

[6] 전용희, “지능형 전력망(Smart Grid)과 정보보호”, 정보보호학회지, 제19권 제4호, pp.65-71, 2009. 8.

[7] 박대우, “VoIP 서비스의 도청 공격과 보안에 관한 연구”, 한국컴퓨터정보학회논문지, 제 11권 제 2호, pp.155-164, 2006. 9.