한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Grid에 사용된 Bluetooth 전기IT기기에 대한 공격 분석

송진영°, 박대우*, 김응식**
°*호서대학교 벤처전문대학원, **호서대학교
e-mail: jedisong@naver.com, prof1@paran.com, eskim@hoseo.edu

Attack Analysis of Bluetooth Electrical IT equipment in Smart Grid

Jin-Young Song°, Dea-Woo Park*, Eung-Sik Kim**
°*Hoseo Graduate School Of Venture, **Hoseo University

● 요 약 ●

Smart Grid에 사용되는 전기IT기기에서 Bluetooth의 보안 취약점이 발견되고 있다. 특히 전기안전을 위한 감시센서 정보전달을 맡고 있어서 위험성은 더욱 커진다. 본 논문은 Bluetooth가 탑재된 전기IT기기에 대한 Hacking Tool 분석을 실시하고, Bluetooth 취약점을 이용한 DoS, Sniffing공격 등 Tool 공격을 실행하고, Smart Grid와 U-IT 전기기기와 전력망에 대한 보안 방안 제시를 한다.

키워드: 지능형 전력망(Smart Grid), 블루투스(Bluetooth), 전기IT기기(Electrical IT Equipment), 해킹(Hacking)

I. 서론

Smart Grid는 기존 전력망에 IT기술을 접목해 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하고자 하는 차세대 전력망을 말한다.

Smart Grid에 사용되는 IT 전기기기에서 Bluetooth는 전기안전을 위한 감시센서 정보전달을 맡고 있어서, 위험성은 더욱 커진다. 특히 WallPad, 지능형 계량기, 아울렛, 수배전반 센서를 통해 전기, 가스, 수도를 검침하려면, WiFi, WiMax, 3G, TDMA/CDMA, RFID, Bluetooth 통신과 같은 여러 형태의 무선망 및 고속 인터넷 백본망이 통합된 통신 형태로 Smart Grid의 전력망 안정성, 장비 상태 감시, 에너지 관리 정책 지원 등을 위한 센싱 및 측정 기술에 포함된 부품이다.

그러나 무선 통신 기술은 무선이라는 통신환경이기 때문에 유선에 비해 보안상으로 매우 취약한 면을 보이고 있다. Bluetooth 전기기기를 통한 취약점 등을 이용, 해킹하여 Bluetooth 전기기기의 권한을 획득[1]한 후 U-Home Gateway를 통하여 Smart Grid를 접속하여, 전력 인프라를 통한 국가 전체 전력 인프라 망을 공격 할 수 있는 가능성이 있다.

본 논문에서는 Bluetooth 공격도구를 연구하고, Bluetooth가 탑재된 IT 전기기기에 대한 Hacking Tool 분석을 실시하고, Bluetooth 취약점을 이용한 DoS, Sniffing공격 등 Tool 공격을 실행하고, Smart Grid와 U-IT 전기기기와 전력망에 대한 보안 방안 제시를 한다.

II. 관련 연구

2.1 Smart Grid 정의

Smart Grid에서 중앙 집중형, 일방향인 전력 계통의 비효율성을 극복하기 위한 것으로, 분산 전원 시스템을 핵심 개념으로 한다. 신재생 에너지를 중심으로 하는 다양한 분산 전원이 도입되어 전력계통을 규모에 따라 분산적이고 독립적으로 운영할 수 있는 유연한 형태를 갖추게 되며, 각 계통에 센서, 미터들을 장착하여 소비자의 요구에 실시간으로 반응하는 지능화된 전력망이다.

그림 1. Smart Grid 개요도
Fig. 1. Overview of Smart Grid

전력 산업의 패러다임이 양에서 질로 공급 중심에서 수요 중심으로 중앙 집중에서 지역 분산으로 전기IT 기술로 변화하는 것을 의미한다. 미래의 전력망이 분산된 네트워크 구조를 가진다는 점에서 Smart Grid는 에너지 분야의 인터넷과 같은 역할을 수행한다고 볼 수 있다[2].

2.2 Bluetooth 무선 통신

2.2.1 Bluetooth 정의

블루투스(Bluetooth)는 1994년 에릭슨이 최초로 개발한 개인 근거리 무선 통신(PANs)을 위한 산업 표준이다. IEEE 802.15.1 규격을 사용하는 Bluetooth는 PANs(Personal Area Networks)의 산업 표준이다. Bluetooth는 다양한 기기들이 안전하고 저렴한 비용으로 전 세계적으로 이용할 수 있는 라디오 주파수를 이용해 서로 통신할 수 있게 한다.

Bluetooth는 유선 USB를 대체하는 개념이며, 와이파이(Wi-Fi)는 이더넷(Ethernet)을 대체하는 개념이다. 암호화에는 SAFER(Secure And Fast Encryption Routine)+을 사용한다. 장치끼리 믿음직한 연결을 성립하려면 키워드를 이용한 페어링(paimg)이 이루어지는데, 이 과정이 없는 경우도 있다[3].

2.3 Bluetooth 공격기법

Bluetooth는 보안 기능을 제공하고 있지만 Dos공격, 도청, MITM공격, 메시지 변조 등과 같은 공격에 여전히 취약하며 Bluetooth 특성을 이용하여 발생되는 공격도 존재한다. 이 장에서는 최근 이용되고 있는 Bluetooth 공격도구를 소개하고자 한다[4].

2.2.1 Blooover

Blooover는 휴대 단말 전용기에 보안 감사를 한다. 통화 점검 등 알려진 취약점 또는 BlueSnarf, 제한된 BlueBug 공격 등을 할 수 있다. BlueSnarfing 공격은 상대방 휴대 단말기를 검색 후 원격제어를 통해 그림, 일정, 전화번호, SMS 등을 알 수 있다[5].

2.2.2 BackTrack

BackTrack은 Slax 기반의 리눅스 배포판으로서 Live-CD나 Download로 제공된다. BackTrack은 디스크 보안관련, 네트워크 분석도구, 포렌식, BlueTooth공격툴(BlueSnarf, BlueBug)등을 포함하고 있다.

2.2.3 BlueSnarf, BlueSnarf++

BlueSnarf는 가장 잘 알려진 블루투스 공격의 형태이다. 공격자는 원래 다른 개체와 명함을 교환하기 위해 개발된 OBEX Push Profile(OPP)을 사용한다. 대부분 이 서비스는 인증이 필요하지 않는다.

공격자는 파일 시스템의 모든 파일을 볼 수 있고, 심지어 파일을 삭제할 수도 있다. 또한 공격자는 메모리스틱 또는 SD 카드와 같은 메모리 확장 카드를 포함한 디바이스에 설치된 메모리에 명령어를 실행시킬 수 있다.

2.2.4 BlueBug

이 취약점은 Bluetooth가 강화된 디바이스에 인증되지 않은 동작을 공격자가 실행할 수 있게 한다. 적절한 환경에서 BlueBug 공격은 단 몇 초 만에 성공할 수 있다. 희BlueBug는 Bluetooth 프로토콜인 L2CAP내의 RFCOMM를 통해 연결과 동시에 상대방 Bluetooth 장치를 제어 할 수 있다. BlueBug 툴은 전화걸기, 불특정 번호를 SMS 전달, 상대방 SMS 읽기등 상대방 Bluetooth가 탑재된 휴대단말기를 제어 할 수 있다.

2.2.5 Bluejacking

해커가 보안이 않된 Bluetooth 디바이스에 익명으로 접속한 다음, 데이터를 빼돌리거나 감염시키는 공격이다. 공격자가 트로이목마 프로그램 등을 심어놓으면 휴대폰 통제권을 얻을 수 있다[6][7].

III. Bluetooth 전기IT기기 분석

3.1. Bluetooth 전기IT기기

특히 가정의 Smart Grid를 적용 할 시에 Bluetooth 활용도 예를 보면 크게 세 가지로 볼 수 있다. 첫번째는 전기, 가스 검침 및 안전 인프라이다. Bluetooth로 신원을 확인해 출입문을 개폐할 수도 있고 WallPad, 아울렛, 수배전반 센서를 통해 전기, 가스, 수도를 검침할 수 있다. 두번째는 전력 통신 기기 리모콘 응용이다. 가정 내의 Bluetooth가 탑재된 A/V기기를 동작제어 할 수 있을 뿐만 아니라 조명기구, 조리기구, 난방장치 제어 그리고 백색가전 제품 동작제어 및 상태를 확인 할 수 있다.

그림 2. 홈 전기IT기기와 Bluetooth
Fig. 2. Home electricity IT equipment and Bluetooth

세번째로는 가정 통신 기기 응용이다. 휴대폰, SmartPhone, 무선 헤드셋 등을 이용하여 가족 간 개인통신 및 인터넷접속을 할 수 있다. 컴퓨터의 경우 마우스 키보드등 주변기기에 Bluetooth를 탑재하여 보다 공간적으로 활용도를 높였다.

특히 WallPad와 같은 지능형 계량기는 WiFi, WiMax, 3G 셀

룰러, TDMA/CDMA, RFID, Bluetooth 통신과 같은 여러 형태의 무선망 및 고속 인터넷 백본망이 통합된 통신 형태로 Smart Grid의 전력망 안정성, 장비 상태 감시, 에너지 관리 정책 지원 등을 위한 센싱 및 측정 기술이 필요하다. 이러한 센서 기술로 인하여 효율적인 전기 사용, 실시간 감시 체계를 제공할 수 있다 [8][9][10].

3.2 Bluetooth 전기IT기기 인증

3.2.1 Bluetooth 키 관리(Key Management)

Bluetooth에서는 안전한 전송을 위해서 여러 종류의 키를 사용한다. 그 중 가장 중요한 요소는 블루투스 기기간의 인증을 위해 사용되는 링크키이다. 이 링크키를 사용하여 암호키를 유도한다. 블루투스의 키 관리는 카-제어과정에서 다음 세 가지의 키를 사용한다.

첫 번째로 사용자 또는 기기가 개인-식별번호를 등록한다. 개인-식별번호(Personal Identification Number, PIN)는 사용자가 선택하며 45비트로 구성되어야 한다.

두 번째로 기기가 개인-링크키를 발생하고 두 번째 기기와 인증과정을 거친다. 블루투스 기기는 인증키(Authentication Key)로 불리는 네 가지의 서로 다른 종류의 링크키(Link Key) 중에서 하나를 사용한다. 네 가지는 임시 번호이거나 반영구적인 128비트의 불규칙한 번호이며, 전송 시마다 새롭게 생성된다.

마지막으로 기기가 링크키로부터 개인 암호화키를 생성하고 두 번째 기기와 인증하는 과정을 거친다. 개인용 인증키(Pricate Encryption Key)와 암호화키(Encryption Key)는 현재 사용되고 있는 링크키로부터 생성된다. 인증키는 암호화가 필요할 때마다 자동적으로 변경되며 8비트와 128비트 사이의 크기를 가진다.

3.2.2 기기 인증(Device Authentication)

Bluetooth의 인증 방식은 Challenge-Response 방식으로서 상대방의 식별 비밀키(대칭키)를 알고 있는지를 확인하기 위해 2-move 프로토콜을 사용한다.

이 프로토콜에서는 양쪽 Bluetooth 기기 모두 같은 키를 갖고 있는지를 확인하고 같은 키를 갖고 있을 때 인증이 성공하게 된다. 반면, 각 기기가 키를 모른다면 연결은 취소된다. 인증 과정 중에 ACO(Authenticated Cipering Offset)값을 생성하여 양쪽 기기가 저장하는데, 이 ACO값은 후에 암호키를 생성하는데 사용된다. 인증이 실패되었을 경우 다시 인증을 시도하는 데는 대기시간(Waiting Time)이 소요된다.

3.2.3 Bluetooth 인증

Bluetooth의 인증 프로시저는 Chllenge-response 형태이다. 즉, 클라이언트가 인증을 받기 위해 서버에 접속을 하면 서버는 바이트 스트링인 Challenge 메시지를 랜덤하게 생성해서 클라이언트에게 전송한다. 클라이언트는 Challenge 메시지를 자신이 갖고 있는 패스워드와 결합해서 서버에게 Response를 전송한다. 서버는 Responserk 자신이 인증하고자 하는 사용자의 패스워드와 결합이 된 것인지 검증해서 인증여부를 결정하게 된다.

IV. Bluetooth 전기IT기기에 대한 Hacking과 보안

4.1. Bluetooth 전기IT기기의 취약점 및 공격 분석

Bluetooth 공격 시 그림 4와 같이 4가지의 예측되는 취약점으로 이루어진다.

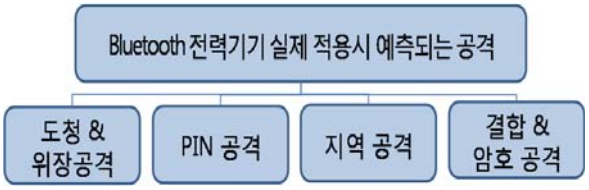

그림 3. Bluetooth 전기기기 취약점
Fig. 3. Bluetooth electrical equipment vulnerability

4.1.1 도청 & 위장 공격

전기 검침 및 전기안전 센서 값에 대한 통신 프로토콜에 사용되는 키 생성 프로토콜이나 키 생성에 대한 프로토콜에 근간하는 Bluetooth의 키 생성 방식은 난수와 PIN 그리고 Bluetooth 디바이스 주소를 이용하여 계산된다. 만약에, PIN이 유효하지 않거나 유닛 간에 전송이 안 된다면 공격자는 이를 쉽게 알아낼 수 있다.

현재 시판된 Bluetooth 헤드셋은 암호화가 안되어 있다. 마스터에서 슬레이브인 Bluetooth 헤드셋 주파수를 검색하여 시간적인 면과 주파수에 일치하는 헤드셋으로 직접 연결하는 방식으로 헤드셋 정보를 입수해 이를 바탕으로 흉내 내어 정보를 탈취 할 수 있다.

4.1.2 결합 & 암호 공격

결합 공격은 공격자가 시간적인 딜레이를 이용하여 디바이스를 추정하여 이루어지는 공격이다. 이는 주파수 도약의 순서를 이용하여 찾아 낼 수 있으며 대응 밴드들에 대해 트래픽의 분석이 이루어지면 더 큰 부분을 얻을 수도 있다.

암호 공격은 공격자가 합산 레지스터와 293의 확률로 결과 값들을 유추해 낼 수 있다. Bluetooth에 대한 공격은 암호의 내부 상태들에 대하여 무작위적 선택을 통해 그에 대응하는 출력키를 얻어 key stream과 key stream간에 보안적 관계를 유추해 보는 공격 방법이다.

암호에 대한 첫번째 공격은 2100비트와 원문의 128비트 보안적 요구사항을 공격하는 공격이다. 이 공격은 LFSR와 덧셈 레지스터의 내용을 추측함으로써 그 결과를 일렬로 관찰하여 LFSR의 내용을 추측하는 공격이다. 두번째의 암호 공격은 생일 공격을 들 수 있다.

4.1.3 PIN 공격

Bluetooth로 신원을 확인해 WallPad, 아울렛, 수배전반 단락 및 제어 디바이스 간에 키를 수립하는 결정에 대한 도청적인 공격을 고려해 볼 수 있다. 이렇게 강탈한 PIN 번호에 대한 정보는 피공격자의 키를 유추할 수 있는 토대가 될 수 있다.

두 디바이스 간에 키를 수립하는 결정에 대한 도청적인 공격을 고려해 볼 수 있다. 이렇게 강탈한 PIN 번호에 대한 정보는 피공

격자의 키를 유추할 수 있는 토대가 될 수 있다.

4.1.4 지역 공격

Bluetooth가 사용하고 있는 전력 통신 기기 리모콘 응용 주파수 매핑 방식에서는 다른 디바이스 간에 의사 랜덤과 서로 다른 상태에서의 주파수를 사용하게 된다.

Bluetooth 구조상으로 슬레이브는 마스터의 주파수를 확인하고 그에 대한 응답을 취하게 되며 마스터의 시간적인 측면과 일치하는 의사 랜덤적인 주파수 매핑 순차를 확정하고 이것에 대한 일치성에 의해 슬레이브는 결과를 전송한다. 공격자는 지리적으로 분산되어 있는 디바이스들에 대한 응답에 대한 결과들을 통해 피공격자와 연결되어 있는 디바이스들을 대상으로 공격을 실시한다.

4.2 Bluetooth 전기IT기기 보안 방법

표 1에서 Bluetooth 전기IT기기에 보안방안을 적용하였다. 64비트로 이루어진 PIN크기를 늘려 안정성을 확보하고 마스터와 슬레이브 간의 주파수 도약 발진기를 거짓으로 만들어 링크키를 보호하도록 관리한다. 이로 인해 다른 장치들이 링크키를 알지 못하게 기밀성을 획득한다. 응용계층에서 공개키 교환과 정책을 통한 상호인증이나 마스터와 슬레이브 사이의 역할에 대한 정책을 통한 인증성을 보장한다.

표 1. 전기IT기기에 대한 공격 분석과 보안방안
Table 1. electricity analysis attacks on IT equipment and security measures

	전기IT기기	보안방안
도청 & 위장공격	전기 검침 및 전기안전 센서 값에 대한 통신 프로토콜	공개키 암호 알고리즘을 통한 기밀성 획득
PIN공격	WallPad, 아울렛, 수배전반 단락 및 제어 디바이스 간	세션키 암호화를 통한 PIN번호 보호를 통해 링크키 생성의 안전성 확보
지역공격	전력 통신 기기 리모콘 응용 주파수 매핑	각 객체 간 서명값을 이용한 인증성 보장
결합 & 암호공격	전기IT기기의 검침 및 개폐 시 신원확인	기존 Bluetooth 암호화 기법을 홈 네트워크의 공개키 암호 알고리즘 적용을 통해 안전한 암호화 획득

V. 결론

최근 Smart Grid의 기술 개발과 유비쿼터스 정보화 사회의 도래로 댁내 전력 사용자는 자신의 사용 전력량과 전기 안전 인프라를 Bluetooth 전기기기를 이용하여 통제, 제어를 할 수 있다. 하지만 Smart Grid에 사용되는 전기IT기기에서 Bluetooth가 전기안전을 위한 감시센서 정보전달을 맡고 있어서 위험성은 더욱 커진다.

본 논문은 Bluetooth가 탑재된 전기IT기기에 대한 Hacking Tool 분석을 실시하고, Bluetooth 취약점을 이용한 DoS, Sniffing공격 등 Tool 공격을 실행하고, Smart Grid와 U-IT 전기기기별로 구분하여 공격을 분석하고 전력망과 시스템에 대한 보안 방안 제시하였다.

참고문헌

[1] 케이벤치, “블루투스 4.0 기술로 무선 의료 및 헬스 기기의 새로운 가능성 열어”, http://www.kbench.com/hardware/?no=101381&sc=1

[2] 전용희, “지능형 전력망과 정보보호”, 정보보호학회, 제19권 제 4호, pp.65~71, 2009. 8.

[3] 박정호, 나경필, 허기중, “차세대 무선 네트웍 기술동향”, 인터넷정보학회지, 제 2권 제 2호, pp.18~24, 2001.

[4] 박대우, 임승린. “해커의 공격에 대한 지능적 연계 침입방지 시스템의 연구”, 한국컴퓨터정보학회, pp.351-360, 2006년 5월.

[5] 천우성, 박대우, “DoS공격에 대한 N-IDS 탐지 및 패킷 분석 연구”, 한국컴퓨터정보학회, 제13권 제6호, pp.217-224, 2008. 11.

[6] 정윤화, 윤주대, 안광선, “Bluetooth 통신을 이용한 홈 오토메이션 보안 시스템”, 한국정보과학회, 제 32권 제 2호, pp.889-891, 2005.

[7] 강태규, 임성수, 김철환, 이기서, “블루투스 스캐터넷을 이용한 물체 인식 시스템에 관한 연구”, 한국철도학회, pp.587-593, 2003.

[8] 이건희 서정택, 이철원, “Smart Grid와 사이버 보안”, 한국통신학회지, 제 27권 제 4호, pp.23~30, 2010.

[9] 박승성, 김종원, 이경일, 권순량, “블루투스를 이용한 홈 네트워크 서비스 설계”, 한국정보과학회, 제 31권 제 2호, 2003.

[10] 최유미. 추현승, “블루투스 단거리 무선 네트워크 상에서 보안과 인증 메커니즘”, 한국인터넷정보학회 춘계학술발표대회, 제5권 제1호, pp 365~368, 2004. 5.