블루투스 보안에 대한 취약점 분석과 대책

지도교수 : 한 상 훈
연 구 자 : 김 형 주

< 목 차 >

요 약

정보통신기술의 비약적인 발달은 오늘날 우리 주변의 사물들을 네트워크로 연결시켜주고 이들에 대한 정보를 언제, 어디서나 쉽게 접할 수 있는 IOT(사물인터넷) 시대의 도래를 촉진하고 있다. IOT(사물인터넷) 서비스는 스마트기기, 센서 등 다양한 단말 및 이기종 네트워크, 애플리케이션 등을 활용한 블루투스를 이용하기 때문에, 그만큼 발생할 수 있는 보안위협도 많을 것으로 예상된다. 본 연구에서는 블루투스를 통한 IOT(사물인터넷) 보안에 대한 취약점을 설명하고, 여기서 발생 가능한 보안위협과 대책에 대해 모색해 보고자 한다.

주요어 : 블루투스(Bluetooth), 사물인터넷(IOT), 해킹(Hacking), 블루본(BlueBorne), 취약점 분석

1. 서론

블루투스는 기본적으로 선을 사용하지 않고 휴대전화/ 휴대용 단말기/ 주변장치 등을 연결하기 위한 기술이다. 오늘날 블루투스는 우리 생활에 깊숙이 자리 잡고 광범위하게 이용되고 있으며 다양한 보안위험에 노출되어 있으나 많은 사람들이 경각심 없이 블루투스를 이용하고 있다는 점에서 블루투스의 보안 위험성 홍보에도 신경 써야 하는 부분이다.

블루투스 취약점은 점점 늘어나고 있다. 그러나 복잡한 블루투스의 특징과 많은 장비의 수 때문에 블루투스 보안은 하기가 어렵다. 블루투스는 근본적으로 IT 기기의 연결 케이블을 없애기 위하여 설계되어있다. 예를 들어, 마우스, 프린터, 휴대전화, GPS 수신기를 케이블로 컴퓨터에 연결할 때 그 컴퓨터는 실질적으로 휴대용기기가 아니다. 또한 컴퓨터는 모든 주변기기를 연결할 충분한 포트가 없다. 그래서 여러 가지 장치들이 작은 규격과 적은 전력으로 접근하기 때문에 높은 수준의 암호화와 인증을 구현하기가 어려워 다양한 위험에 노출될 수 있다.

또한 보안을 하기 위해 많은 노력과 비용이 들지만 공격이 성공하게 되면 굉장히 위험하므로 이러한 위험에 대한 대응책을 찾고자 한다.

본 연구에서는 블루투스 기술이 가지고 있는 취약점과 취약점에 노출되면 어떤 현상들이 나타나는지 알아보고 취약점에 대한 대응책을 찾고자 한다. 본 논문의 구성은 다음과 같다.

본론에서는 첫째, 블루투스와 관련된 해킹 기술을 알아보고 둘째, 블루투스를 통한 IOT(사물인터넷)보안 문제점에 대해 설명하고 셋째, 블루본 에서 적용하고 있는 보안 문제와 해결 방안에 대해 제시한다. 마지막엔 결론으로 본 논문의 끝을 맺는다.

2. 블루투스

2.1 블루투스와 관련된 다양한 해킹 기술

① 블루프린팅(Blueprinting): 블루투스 공격 장치의 검색 활동을 의미한다.

각 블루투스장치는 MAC 주소와 유사하게 6바이트의 고유 주소가 있는데, MAC 주소와 유사하게 앞의 3바이트는 제조사에 할당되고, 뒤의 3바이트는 블루투스 장치별로 할당된다. 그런데 뒤의 3바이트의 주소만으로는 블루투스 장치의 종류를 식별하는 것이 불가능하다.

이 때문에 블루투스 장치는 장치 간 종류(전화통화, 키보드 입력, 마우스 입력 등)를 식별하기 위해 서비스 발견 프로토콜(SDP: Service Discovery Protocol)을 보내고 받는다. 그리고 이 서비스 발견 프로토콜을 이용해 공격자는 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.

② 블루 스나프(BlueSnarf): 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.

공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근할 수 있다.

③ 블루버그(BlueBug): 블루투스 장비 간 취약한 연결 관리를 악용한 공격이다.

공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행하는 공격이다. 블루투스 기기는 한 번 연결되면 이후에는 다시 인증하지 않아도 서로 연결되는데, 이런 인증 취약점을 이용하여 공격하는 것이다. 일부 블루투스 기기에서는 10미터~15미터 정도의 거리에서 블루투스 기기에 전화 걸기, 불특정 번호로 SMS 보내기, 주소록 읽기 및 쓰기 등을 공격자가 실행할 수 있다.

이 공격을 이용해 지하철에서 높은 금액을 과금하는 특정 번호로 행인의 전화로 전화를 걸어 돈을 버는 등의 행위가 발생하기도 했다.

④ 블루 재킹(Bluejacking): 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼뜨리는 것이다.

2.2 블루투스를 통한 IOT(사물인터넷) 보안

2.2.1 IOT(사물인터넷) 보안 위협 발생 원인과 위험성

사물인터넷 시대에는 컴퓨터나 스마트폰 뿐만 아니라 수백억 개에 달하는 다양한 유형의 사물들이 인터넷에 연결된다. 이러한 사물인터넷 디바이스들은 제한된 배터리 용량에 컴퓨팅 파워도 떨어지는 소형의 디바이스인 경우가 대부분이다. 따라서 별도의 암호화 과정 없이 데이터를 생성한 후 주변의 다른 디바이스들을 통해 인터넷으로 전달된다.

이러한 과정에서 악의적인 사용자에 의해 불법적으로 데이터가 수집되거나 변조된다면, 개인의 프라이버시를 침해하는 것뿐만 아니라 심각한 보안사고까지 일으킬 수 있다.

사물인터넷 서비스는 가상세계와 현실 세계를 연결하는 것이기 때문에, 사이버 공간에서의 해킹은 그대로 물리적인 공간의 위험으로 전이될 수 있기 때문이다.

2.2.2 보안 위협의 유형

사물인터넷 보안 위협은 사물인터넷을 구성하는 요소인 디바이스, 네트워크, 서비스 영역에서 모두 발생할 수 있다. 사물 인터넷 보안 위협에는 비인가 접근, 복제 공격, 정보 유출, 데이터 위변조, 서비스 거부, 프라이버시 침해 등이 있다.

구성요소	보안 위협
서비스	데이터 위/변조, 데이터의 기밀성/ 무결성, 프라이버시 침해, 비인가 된 어플리케이션 및 사용자의 접근
네트워크	데이터 위/변조, 인증방해, 신호 데이터의 기밀성/ 무결성 침해, 정보유출, 서비스 거부(DOS)
장치/센서	장치의 기밀성/ 무결성 침해, 비인가 접근, 복제 공격

[표 1] 사물인터넷 구성 요소별 보안 위협

비인가 접근은 권한이 없는 공격자가 특정한 장치나 지원, 서비스에 비인가 된 접근을 시도한 후 그것들을 조작하거나 물리적인 손상을 입히는 보안 위협을 말한다. 이외에도 비인가 접근을 통해 디바이스나 사용자와 관련된 정보가 유출될 수도 있으며, 이는 곧바로 프라이버시 침해 문제를 일으키기도 한다. 또한 디바이스가 생성시키거나 시스템에 의해 가공된 데이터를 변조함으로써 사물인터넷 서비스의 품질을 떨어뜨릴 수도 있다.

대부분 사물인터넷 디바이스들은 무선 통신 기술을 이용하기 때문에, 스마트 디바이스들이 전송하는 데이터를 도청하거나 스니핑 함으로써 해당 디바이스를 복제하는 것도 가능하다.

또한 이렇게 복제한 디바이스를 이용해서 스팸을 발송하거나 대량의 데이터를 생성함으로써 서비스가 제대로 제공되지 않도록 할 수도 있다.

[사진 1] 셋톱박스가 과도한 트래픽을 일으켜 게임 서비스 중단

셋톱박스가 과도한 트래픽을 발생시키도록 함으로써 게임 서비스가 중단된 사례가 있다.

KISA는 최근 A게임사 유럽지사 게임이 DDos공격 대상이 됐다는 신고를 받았다. 게임에 과도한 트래픽을 전송한 국내 IP를 조사한 결과 유수 대학에서 공격이 발생했다. 신고 내용과 IP 등 정황만 놓고 보면 대학 내 좀비PC가 DDos공격을 한 일반적인 경우로 파악됐다.

하지만 실제 조사 결과 공격을 감행한 상당수 장비가 대학 내 설치된 냉난방 관리용 셋톱박스였다. C대기업이 대학 전체 냉난방을 효율적으로 관리하려고 설치한 장비였다.

박○○ KISA 취약점 분석팀장은 “서버나 PC가 아닌 셋톱박스가 공격지가 된 이례적인 사고”라며 “학교나 기업 내 냉난방을 관리 제어하는 기기에 리눅스 등 운영체계(OS)가 들어가고 NTP를 쓰면서 이들 취약점을 악용한 공격이 발생해 주의를 기울어야 한다.”고 말했다.

2.2.3 예상되는 피해

① 자동차: 속도조절, 브레이크, 핸들, 경적 울리기 등 각종조작
② 스마트TV: 디도스 공격으로 TV마비, 내장 카메라 해킹해 사생활 촬영
③ 의료장비: 인슐린 펌프 해킹해 인슐린양 조절, 심박동기 해킹해 박동수 조절
④ 정유시설: 석유 공급량 조절, 잘못된 데이터전송
⑤ 비데: 물세기, 변화온도 조절, 음악재생, 향기발신 등 기능조절
⑥ 스마트홈: 전자도어록과 보안카메라 해킹해 무방비 상태로 만듦
⑦ 웨어러블컴퓨팅: 정보조작으로 잘못된 정보 인지

2.2.4 위험요소와 원인

유형	주요제품	주요 보안위협	주요 보안위협 원인
멀티미디어 제품	스마트TV, 스마트 냉장고 등	1. PC 환경에서의 모든 악용 행위 2. 카메라/마이크 내장 시 사생활 침해	1. 인증 메커니즘 부재 2. 강도가 약한 비밀번호 3. 펌웨어 업데이트 취약점 4. 물리적 보안 취약점
생활가전 제품	청소기, 인공지능 로봇 등	1. 알려진 운영체제 취약점 및 인터넷 기반 해킹 위협 2. 로봇청소기에 내장된 카메라를 통해 사용자 집 모니터링	1. 인증 메커니즘 부재 2. 펌웨어 업데이트 취약점 3. 물리적 보안 취약점
네트워크 제품	홈 캠, 네트워크 카메라 등	1. 사진 및 동영상을 공격자의 서버 및 이메일로 전송 2. 네트워크에 연결된 홈캠 등을 원격으로 제어하여 임의 촬영 등 사생활 침해	1. 접근통제 부재 2. 전손데이터 보호 부재 3. 물리적 보안 취약점
제어 제품	디지털 도어락, 가스밸브 등	1. 제어기능 탈취로 도어락의 임의 개폐	1. 인증 메커니즘 부재 2. 강도가 약한 비밀번호 3. 접근통제 부재 4. 물리적 보안 취약점
	모바일 앱(웹) 등	1. 앱 소스코드 노출로 IOT제품 제어기능의 탈취	1. 인증정보 평문 저장 2. 전송데이터 보호 부재
센서 제품	온/습도 센서 등	1. 잘못된 또는 변조된 온/습도 정보를 전송	1. 전송데이터 보호 부재 2. 데이터 무결성 부재 3. 물리적 보안 취약점

[표 2] 위험요소와 원인

3. 본론

3.1 블루투스를 통한 IOT(사물인터넷) 기기 공격

블루투스 취약점은 안드로이드, 윈도우, 리눅스, 그리고 버전 10 이전의 iOS 등에서 발견됐다. 공격자는 이 취약점을 통해 사용자 인터랙션 없이도 기기들을 광범위하고 빠르게 감염시킬 수 있으며, 심지어 망이 분리된 기기들까지 감염시킬 수 있는 것으로 나타났다.

아미스는 자사가 발견한 제로데이 취약점 8개를 묶어 '블루본(BlueBorne)'이라고 명명했다.

3.1.1 블루본 취약점

CVE 번호	취약점 요약
CVE-2017-0781	안드로이드 BNEP(Bluetooth Network Encapsulation Protocol, 테더링)에서 발생하는 원격코드실행 취약점
CVE-2017-0782	안드로이드의 BNEP PAN(Personal Area Networking, IP기반 장치간 네트워크 연결) 프로필에서 발생하는 원격코드실행 취약점
CVE-2017-0783	안드로이드 블루투스의 PAN 프로필에서 발생하는 Man-in-the-Middle 공격 취약점
CVE-2017-0785	안드로이드 SDP(Service Discovery Protocol, 주변 장치 식별)에서 발생하는 정보노출 취약점
CVE-2017-8628	윈도우의 블루투스 드라이버에서 발생하는 스푸핑 취약점
CVE-2017-1000250	리눅스 블루투스 스택(BlueZ)에서 발생하는 정보노출 취약점
CVE-2017-1000251	리눅스 커널 원격코드실행 취약점
CVE-2017-14315	애플의 Low Energy 오디오 프로토콜에서 발생하는 원격코드실행 취약점

[표 3] 블루본 취약점

3.1.2 안드로이드 취약점

① 정보 유출 취약점 (CVE-2017-0785)

Android 운영체제의 첫 번째 취약점은 공격자가 아래에 설명된 원격 코드 실행 취약점 중 하나를 활용하는 데 도움이 되는 유용한 정보를 제공하는 것이다.

이 취약점은 SDP (Service Discovery Protocol) 서버에서 발견되었으므로, 장치가 주변의 다른 Bluetooth 서비스를 식별할 수 있다. 이 결함은 침입자가 일련의 정교한 요청을 서버에 보내어 응답으로 메모리 영역을 노출하게 한다. 이러한 정보는 이후, 보안 대책을 우회하여 장치를 제어하기 위해 공격자가 악용할 수 있다. 또한 이 취약점을 통해 침입자는 대상 장치에서 암호화키를 유출하고 블루투스 통신을 도청할 수 있다.

② 원격 코드 실행 취약점 (CVE-2017-0781)

이 취약점은 Bluetooth 네트워크 캡슐화 프로토콜 (BNEP) 서비스에 있으며, Bluetooth 연결 (테더링)을 통한 인터넷 공유가 가능하다.

BNEP 서비스의 결함을 통해 메모리의 외부적인 손상을 초래할 수 있다. 이는 쉽게 악용되어 장치에서 코드를 실행하여 효과적으로 제어할 수 있다. 적절한 권한 검증조치가 부족하여 이 취약점을 유발하는 데 사용자 상호 작용, 인증 또는 페어링이 필요하지 않으므로, 사용자는 발생 중인 공격을 전혀 알지 못한다.

③ 원격 코드 실행 취약점 (CVE-2017-0782)

이 취약점은 이전과 유사하지만 상위 수준의 BNEP 서비스인 PAN(Personal Area Networking) 프로파일에 상주하며 두 장치 간에 IP 기반 네트워크 연결을 설정한다. 이 경우 메모리 손상은 더 커지지만 공격자가 감염된 장치를 완전히 제어할 수 있다. 이전 취약점과 마찬가지로, 사용자 상호 작용, 인증 또는 페어링 없이도 트리거가 될 수 있다.

④ 블루투스 파인애플 – 중간 공격자 (CVE-2017-0783)

Man-in-the-Middle (MiTM) 공격은 침입자가 대상 장치에서 오고 가는 모든 데이터를 가로채고 개입할 수 있도록 한다.

Wi-Fi를 사용하여 MiTM 공격을 생성하려면 침입자는 특수 장비 및 대상 장치에서 열린 Wi-Fi 네트워크로의 연결 요청이 필요하다. 블루투스에서 공격자는 블루투스 기능이 있는 모든 장치를 사용하여 적극적으로 목표에 참여할 수 있다.

취약점은 블루투스 스택의 PAN 프로필에 있으며 공격자가 대상 장치에 악의적인 네트워크 인터페이스를 만들고 IP 라우팅을 다시 구성하며 장치가 악의적인 네트워크 인터페이스를 통해 모든 통신을 전송하도록 한다. 이 공격은 사용자 상호 작용, 인증 또는 페어링을 요구하지 않으므로 실제로 보이지 않게 된다.

3.1.3 윈도우 취약점

① 블루투스 파인애플 – 중간 공격자 (CVE-2017-8628)

이 취약점은 Android 운영 체제에서 발견된 것과 동일하며 일부 블루투스 프로토콜을 구현할 때 동일한 원칙을 공유했기 때문에 두 시스템에 영향을 미친다. 블루투스 스택에 존재하며 공격자가 피해자의 장치에 악의적인 네트워크 인터페이스를 만들고 IP 라우팅을 다시 구성하며 장치가 모든 통신을 통해 강제로 전송하도록 한다.

이 공격은 사용자 상호 작용, 인증 또는 페어링을 필요로 하지 않으므로 실제로 보이지 않는다.

3.1.4 Linux 취약점

① 정보 유출 취약점 (CVE-2017-1000250)

Android 정보 유출 취약점과 마찬가지로, 이 취약점은 장치 주변에서 Bluetooth를 사용하는 다른 서비스를 식별하는 SDP 서버에 있다. 이 결함은 침입자가 일련의 정교한 요청을 서버에 보내어 응답으로 메모리 비트를 노출하도록 하여, 블루투스 통신의 암호화키를 포함할 수 있는 블루투스 프로세스의 중요한 데이터를 노출하는데 악용될 수 있다.

② BlueZ의 스택 오버플로우 (CVE-2017-1000251)

이 취약점은 운영체제의 핵심인 Linux 커널의 블루투스 스택에서 발견되었다. 두 장치를 연결하는 데 사용되는 L2CAP(논리 링크 제어 및 적응 프로토콜)의 내부 결함으로 인해 메모리 손상이 발생한다. 공격자는 이 메모리 손상을 통해 장치를 완벽하게 제어할 수 있다.

3.1.5 iOS 취약점

Apple의 저에너지 오디오 프로토콜 (CVE-2017-14315)을 통한 원격 코드 실행

이 취약점은 LEAP (Low energy audio protocol)라고 불리는 Bluetooth를 기반으로 작동하는 Apple이 고안한 새로운 프로토콜에서 발견되었다. 이 프로토콜은 저에너지 오디오 주변 장치 (예: 저에너지 헤드셋 또는 Siri Remote)로 오디오를 스트리밍하도록 설계되었다. 이렇게 하면 블루투스 저에너지 (Bluetooth Low Energy) 장치만 오디오를 스트리밍하고 오디오 명령을 보낼 수 있다. LEAP 구현의 결함으로 인해 대용량 오디오 명령을 대상 장치로 보내고 메모리 손상을 초래할 수 있다.

LEAP를 통해 전송된 오디오 명령의 유효성이 제대로 검증되지 않기 때문에 공격자는 메모리 손상을 사용하여 장치를 완전히 제어할 수 있다.

3.2 블루본 버그

3.2.1 취약성의 위험

아미스에 따르면, 블루본 버그가 손상을 입히는 범위는 상당히 다양하다.

즉, 블루본 버그가 확산되면 네트워크 방어벽에서 가장 취약한 부분을 표적으로 삼는다. “블루본 버그는 상당히 감염성이 높다”고 아미스는 덧붙였다. 따라서 랜섬웨어와 데이터 절도, 사이버 간첩행위 등을 포함한 여러 가지 악의적인 목표를 가지고 이 버그를 사용할 수 있다.

3.2.2 블루본 버그는 어떻게 작동 하는가?

블루본 버그는 다른 사이버 공격과는 달리 블루투스에 연결된 기기를 표적으로 삼는다. 즉, 블루투스 소프트웨어의 약점을 공략해 프린터와 휴대폰, 스마트 TV, 컴퓨터로 침입 하는 것이다. 공격자가 거리에서 블루본 버그에 취약한 사람 곁을 스쳐 지나가기만 해도 감염될 수 있다고 아미스는 설명했다. 바로 이것이 많은 사람들이 자신도 모르는 새 블루본에 감염될 수 있는 이유다.

3.2.3 공격이 멀리, 빠르게 확산되는 이유?

블루투스는 단거리 통신에서 가장 광범위하고 선두적인 프로토콜이기 때문에 블루투스에 연결된 수십억 대의 기기가 블루본 버그의 공격에 노출돼 있다. 그리고 모바일 기기와 스마트워치, 자동차까지 거의 모든 종류의 IOT 기기가 블루투스를 사용하고 있다는 특성도 있다. 심지어 병원에서도 의료 기기에 블루투스를 활용하고 있다.

3.2.4 블루본 버그 공격으로 IOT(사물인터넷) 보호

보안회사의 연구진들은 새로운 방법을 사용해 블루본의 취약점을 확산할 수 있다는 사실을 밝혀냈다. 모바일 데이터 관리와 종점 보호, 네트워크 보안 솔루션과 방화벽 같은 기존의 보안 조치로는 블루본 버그에 효과가 없다. 이러한 기존의 보안 조치는 모두 인터넷 기반 위협에 대처할 수 있는 방법이기 때문이다.

따라서 블루본 버그로부터 보호하기 위해서는 아래와 같은 솔루션을 제시한다.

① 꼭 필요한 경우가 아니라면 기기에서 블루투스를 비활성화해야 한다. 사용을 마친 즉시 전원을 꺼야 한다.
② 현재 보유하거나 네트워크에 연결된 장치를 식별해야 한다. 장치 제조사를 파악하여 기기를 업데이트해야 한다.
③ 업데이트가 제공되는 즉시 시스템 패치를 적용해야 한다.

4. 결론

블루투스 통신이 보편화됨에 따라 IOT(사물인터넷) 시대에 도래한 만큼 여러 가지 취약점 및 유형으로 알 수 있듯이 보안위협은 앞으로 더욱 더 진화하며 우리 생활 속 깊이 영향을 미칠 것이라고 생각한다. 이러한 위험 요소 위협에서 최소한의 방어 할 수 있는 대책을 제시하고자 한다.

① 모든 기기의 암호는 기본 값에서 변경해야 한다. 권한은 기기가 역할을 할 수 있는 범위 내에서 최소한으로 해야 한다.
② 블루투스 기능은 사용하지 않을 경우 비활성화 해야 한다.
③ 와이파이 네트워크를 자동으로 제공하는 기기가 있는지 점검해서 사용하지 않는 것이 좋다.
④ 블루투스와 주고받는 데이터를 암호화하는 기능이 지원한다면 바로 사용해야 한다.
⑤ 업데이트는 매달 직접 확인하거나 기기가 자동으로 업데이트 하든 패치를 계속해서 적용해야 한다. 업데이트를 받을 수 없는 기기는 사용하지 않는 것이 좋다.
⑥ 제조업체가 더 이상 기술지원이나 보안을 제공하지 않는 기기를 사용하지 않아야 한다.

블루투스 통신은 이제 우리 생활에서 없어서는 안 되는 통신기기가 되었다. 좀 번거롭더라도 경각심을 가지고 신경 써서 대처한다면 위험 요소로부터 조금은 자유로워 질 수 있다고 생각한다. 이러한 방법으로 모든 위험요소에서 자유로울 수는 없지만 많은 위험 요소들 중 일정 부분은 방어할 수 있는 대책이 될 수 있을 것이라고 생각한다.

참고문헌

1) 출처: 블루투스의 취약점과 위협 (정보 보안 개론, 2013. 6. 28., 양대일)
2) 출처: 사물인터넷 보안 [Securing the Internet of Thing] (ICT 시사상식 2017, 2016.12.20)
3) 출처: KISA, 보안공지, BlueBorne 블루투스 공격 관련 보안 업데이트 권고 (2017.09.14.)
4) 출처: KISA, 기술안내서 가이드, 홈・가전 IoT 보안가이드(2017.8.7.)
5) 출처: AI타임즈, 블루투스를 통해 IoT 기기를 공격, 조종하는 '블루본 버그' (2019.03.29.)
6) 출처: 사물인터넷 보안 기술 (국립중앙과학관 - 사물인터넷)
7) 출처: ETNEWS, [정보보호] IoT 보안위협 현실화... 냉난방 셋톱박스 DDoS 공격에 악용(2014.5.18.)