정 보 보 호 학 회 지
제26권 제3호, 2016. 6

저전력 블루투스(BLE) 비콘 보안 취약점 연구

김 승 일*, 지 선 학**, 이 재 우***

요 약

최근 사물인터넷(IoT) 시장의 급격한 성장과 함께 적용 서비스 분야도 급격하게 늘어나고 있다. 다양한 객체와 인터넷의 연결로 무수히 많은 서비스가 제공되고 있으며 기업 및 공공기관은 이를 활용하여 다양한 콘텐츠를 개발하고 있다.

하지만 IoT인프라의 급격한 범위 확장 및 활용 표준화가 이루어지지 않았고, 이에 따라 인프라 프로세스의 혼란을 야기할 수 있다. 이는 내·외부적인 위협의 증가로 이어진다. 따라서 사물인터넷 기술이 현재 시장보다 활성화 되고 실 서비스 적용 분야가 증가할수록 제도적, 물리적, 기술적인 취약점이 원인이 되어 공격자는 사물인터넷 단말기 내부에 악성코드를 심어 원격 통제를 하거나, 일정 무선 주파수를 동기화 하여 스니핑이나 스푸핑 등의 공격으로 데이터 변조의 위협이 존재한다.

본 연구를 통해 콘텐츠 정보제공의 주 목적으로 활용되는 미들웨어장비인 Bluetooth 4.0 기반의 저전력 비콘(Beacon)의 기능을 활용한 서비스에서 발생될 수 있는 내재적 위협으로부터 정책적, 기술적, 물리적 통제 및 대응 방안을 제안하였다.

Ⅰ. 서 론

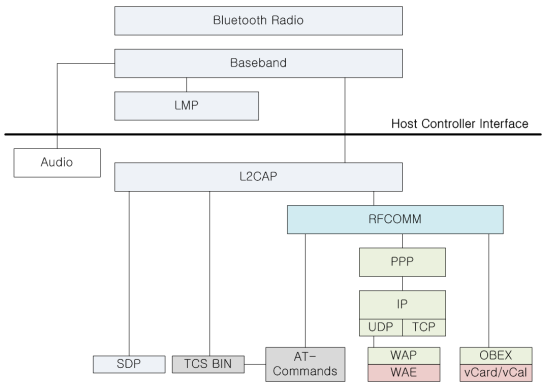
IT산업의 큰 이슈인 IoT(Internet of Things)는 여러 분야에 다양한 용도로 활용되고 있다. 이는 ICT(Information Communications Technologies) 환경의 폭발적인 성장에 기반 한다. 다양한 객체와 인터넷의 연결로 무수히 많은 서비스가 제공되고 있으며 기업 및 공공기관은 이를 활용하여 다양한 콘텐츠 개발이 이루어지고 있다. 특히 모바일과 연계된 무선 통신 사업에 가장 활발한 적용이 이루어지고 있다. 무선 통신 사업에 활용되고 있는 중요한 기술 중에 하나는 블루투스(Bluetooth) 무선 통신 기술이다. 이 중 본 논문에서 다루게 될 불루투스 기술 기반의 비콘은 현재 여러 IT 산업에서 활용 되고 있다. 하지만 이러한 비콘 기술은 블루투스 기반의 서비스이기에 기존의 블루투스 통신 기술 자체의 보안 취약점을 가지고 가게 된다.

이에 따라 본 논문에서는 이러한 IoT 환경에서의 저전력 블루투스 기술 기반의 비콘을 소개하고 국내·외 동향, 블루투스의 보안기술 및 취약점, BLE(Bluetoot Low Energy)기반의 비콘(Beacon)의 취약점 등을 통하여 이에 대한 대응방안의 도출한다.

Ⅱ. 블루투스(Bluetooth) 기술

2.1. 블루투스 프로토콜

- Host Controller Interface : 호스트 컨트롤러에 포함된 베이스밴드나 링크 매니저, 그리고 하드웨어 등을 접근하고 제어하기 위한 표준화된 인터페이스를 의미한다. 만약 이런 표준화된 인터페이스를 제공하지 않는다면 베이스밴드 프로세서나 블루투스 칩셋 등



〔그림 1〕 블루투스 프로토콜 스택

* 동국대학교 정보보호학과 석사과정
** 동국대학교 정보보호학과 석사과정
*** 동국대학교 국제정보대학원 석좌교수

으 하드웨어 벤더에 따라 하위 계층 프로토콜의 인터페이스 방법이 달라질 것이다. 이로 인해 하드웨어에 따라 애플리케이션을 따로 제작해야 하는 번거로움이 생기게 된다.[1]

- L2CAP : 상위 계층 프로토콜과 HCI, 베이스밴드 등의 하위 프로토콜 사이에서 중재 조정 역할을 한다. 주요 역할은 프로토콜 멀티플랙싱, 분할 및 재조합을 담당한다.[1]
- SDP : 연결된 블루투스 장치에서 어떠한 서비스가 가능하고, 그 가능한 서비스의 특지에 대한 정보를 교환하기 위한 프로토콜이다. SDP는 서버-클라이언트 구조로 서버 장치는 가능한 서비스 목록과 각 서비스에 대한 세부사항을 데이터베이스로 가지고 있다가 클라이언트의 요청에 의해 해당 정보를 전송한다.[1]
- RFCOMM : RS-232 시리얼 포트를 에뮬레이션하는 역할을 담당한다. RFCOMM은 스펙 상 동시에 60개의 포트를 열 수 있는 다중 에뮬레이션(Multiple Emulation)을 지원하며 각 포트는 DLCI(Data Link Connection Identifier)라는 고유한 인자를 지니고 있다. 이러한 다중 에뮬레이션은 두 개의 블루투스 디바이스 사이에서 다중 시리얼 포트를 에뮬레이션 할 수도 있지만, 여러 개의 블루투스 디바이스와 다중 시리얼 포트 에뮬레이션을 하는 것도 가능하다.[1]

2.2. 블루투스 보안 매니저

블루투스는 링크레벨에서 보안 매니저를 통해 블루투스 장치 및 서비스에 대한 제어 권한을 통제하며 블루투스의 모든 보안관련 처리는 보안 매니저에서 담당한다. 보안 매니저의 주요 특징은 다음과 같다.

- 서비스 관련 보안 정보 관리
- 장치관련 보안 정보 관리
- 프로토콜 및 응용프로그램의 보안관련 질의응답
- 인증 및 암호화 수행

일반적인 연결설정 과정 중 보안 관련 절차를 살펴보면 L2CAP의 연결 요청을 받아 보안 매니저에게 접근 허용 여부를 질의하며, 서비스 DB와 디바이스 DB를 조사를 통해서 필요한 인증 및 암호화를 수행한다.[2]

2.2.1. 블루투스 보안 레벨

- 장치 신뢰 레벨 관리
  1) 신뢰 장치(Trusted Device) : 인증된 장치이며 링크키가 저장되어 있고 디바이스 DB에 “Thrusted"로 정의된 장치이다.
  2) 비 신뢰 장치(Untrusted Device) : 기 인증된 장치이며 링크키가 저장되어 있지만, 디바이스 DB에 "Trusted"로 정의되지 않은 장치이다.
  3) 알려지지 않은 장치(Unknown Device) : 보안 관련 정보가 없는 장치이다.
- 블루투스 보안 모드
  1) Security Mode 1 : 보안기능을 제공하지 않는 모드이다. 블루투스 장치는 ‘Promiscuous' 상태로 다른 장치와 별도의 보안 기능이 적용되지 않는 상태에서 연결 및 접근을 허용한다.
  2) Security Mode 2 : 서비스 레벨 보안 모드이며 LMP 링크 연결이 완료되고, L2CAP 채널이 연결되기 이전에 도작한다. 보안 매니저는 특정 서비스나 장치의 접근을 허용할 것인지 결정하는 형태로 제공한다.
  3) Security Mode 3 : 링크 레벨 보안 모드이다. 물리적인 링크가 완전히 설정되기 전에 동작한다. 이 모드에서는 모든 장치간의 연결에 대해서 인증 및 암호를 기능을 적용한다.
  4) Security Mode 4 : Security Mode 2와 유사한 서비스 레벨 보안 모드이다. Security Mode 2 보다 보안기능을 강화하면서 페어링을 단순화하기 위해 SSP(Secure Simple Pairing)를 적용하였다. SSP는 키 교환 및 링크 키 생성을 위해 ECDH(Elliptic Curve Diffie Hellman)기법을 이용하였다.[3]

2.2.2. 인증

블루투스 인증 절차는 요구자(Claimant)와 검증자(Verifier)로 구성된 Challenge-Response형태를 취하게 된다. 요구자는 검증자에게 자신을 증명하도록 시도하고, 검증자는 요구자의 증명을 검증하기 위해 링크키를 이용한다.[3]

2.2.3 기밀성

블루투스는 인증과 더불어 상호간에 주고받는 데이터의 도청을 방지하기 위해서 데이터 암호화 기능을 제공한다.[3]

2.3. 블루투스 취약점

- Bluetooth Scanner : 블루투스 단말기의 취약점을 공격하기 위해서 주변 지역에 블루투스 지원 단말기를 스캔하는 공격으로 단말기의 프로파일을 탐색하여 지원 서비스를 확인하는 단계가 우선적으로 이뤄진다. 즉, 발견된 장치에 대한 정보를 추출하기 위해서 검색하는 기능을 제공한다.
- Bluesnarfing : 펌웨어 취약점을 이용하여 장치 내에 저장된 데이터에 대한 접근을 허용하는 공격이다.
- Bluejacking : 블루투스 지원 단말기에 SPAM이나 피싱 공격을 시도하는 메시지나 파일을 전송하는 공격이다.
- Bluebugging : 펌웨어 취약점을 이용하여 블루투스 지원 장치에 대한 접근 권한을 획득하는 공격이다.
- Denial of Service : 블루투스 지원 단말에 지속적으로 데이터를 전송하여 배터리 소모가 이뤄지게하거나 단말기가 재부팅 되도록 만들어 정상적인 사용을 방해하는 공격이다.[4]

Ⅲ. 비콘(Beacon) 기술

비콘은 최근 IoT산업 시장에서 가장 이슈이며, 적용할 수 있는 서비스가 다양할 것이라고 예측하고 있다. 전통적인 의미에서의 비콘은 어떤 신호를 알리기 위해 주기적으로 전송하는 기기를 모두 의미한다. 따라서 등대나 봉화 같은 것도 전통적인 의미에서는 모두 비콘에 포함된다고 할 수 있다. 이러한 비콘의 개념은 현대에 이르러 IT 기술과 만나 보다 확장되고, 일상 깊숙이 들어왔다. 정밀한 사용자 위치정보기술과 기존 보다 빠른 데이터 전송 및 광범위한 전파 범위로 결제, 광고 등 마케팅 서비스 분야에서 각광받고 있으며, Bluetooth LowEnergy(BLE) 프로토콜 기반의 저전력 근거리 무선통신장치로서 많은 하락이 되어있는 블루투스 시장에 다시 활력을 불어넣을 것으로 기대되고 있다.

〔그림 2〕 비콘 내부 구조

3.1. 블루투스 v4.0기반 비콘 특징

① 소량(168비트=21바이트)의 패킷
② 주기적 신호
③ 페어링 불필요(No Pairing)
④ 저전력(3V 코인, 200~300ms 주기 기준, 약 2년)
⑤ 도달거리 최대 50m, 안정적 20~30m
⑥ UUID+메이저+마이너+RSSI(보내는 신호는 비콘 송신기 ID 값과 수신신호세기(RSSI)가 전부)
⑦ iOS7, 안드로이드 4.3 이상 지원: 60~70% 커버리지
⑧ 블루투스가 켜져 있어야만 신호 수신
⑨ 소형, 설치보다는 부착 개념
⑩ 저비용[5]

3.2. 국내·외 비콘 활용 동향

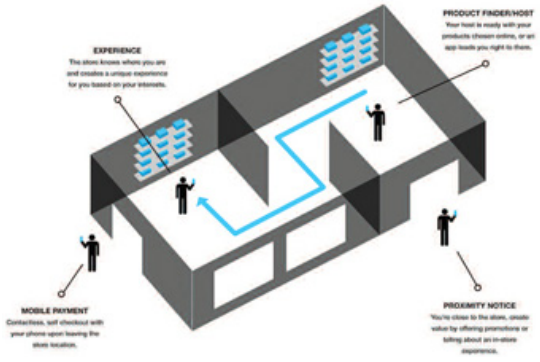
비콘은 국내·외 다양한 산업군에서 활용되고 있으며 특히 해외에서 적극적으로 개발 중이며 적극적인 활용이 기대되고 국내에서도 통신사 및 소셜 마케팅 업체에서 활용하고 있다.

3.2.1. 국내 비콘 활용 동향

BC카드와 롯데카드는 관광객과 멤버십 대상의 비콘 서비스 실시함으로써 국내 관광서비스 질의 향상을 가져왔으며, 외국 관광객의 국내 관광 서비스 만족도 향상에 이바지하였다. 특히, BC카드는 카드업계 최초로 한국을 방문하는 중국인 관광객을 대상으로 비콘(Beacon) 서비스 상용화하여 각종 관광지 정보를 소개하였으며 명동에 있는 유니온 페이카드 VIP 라운지를

방문하면 한국 관광지 소개 및 유니온 페이카드 이벤트 등에 대한 정보 제공하는 서비스를 진행하고 확대하였다.[6]

또한 비콘 서비스를 적극적으로 활용하고 있는 분야가 이동통신사이다. LGU+는 매장별 고유 주파수를 가진 음파를 송출하는 딩동 서비스 출시, 딩동 앱을 실행하고 매장에 들어서면 스마트폰 마이크가 매장 특유의 음파를 인식해 해당 매장의 쿠폰과 이벤트 정보를 실시간으로 제공한다.[7] SK텔레콤은 프로농구단과 함께 비콘을 이용한 실내 위치정보 기반 솔루션 모바일앱 서비스를 제공하여 서울 잠실학생체육관에 블루투스 비콘을 설치 팬들에게 스마트폰으로 실시간 경기 정보 제공하였다. 특히 실내 위치정보를 기반으로 대형 전시장 내의 관람 편의성을 높여주는 모바일 앱 가이드 서비스인 '위즈턴 전시회(Wizturn Exhibition)'를 상용화했고 전시장 및 관람회에 시범활용하여 비콘의 뛰어난 실내 위치정보 기반 기능을 발휘하였다. 전시장 내부에 정확한 실내 측위 구현을 위해 지향성 안테나를 비롯한 SK텔레콤의 독자적인 핵심기술을 적용한 약 600개의 전용 블루투스 비콘을 전시장에 설치, 평균 5미터 이내의 측위 정확도를 확보하여 위치에 따른 관람시설 및 전시장의 정보를 사용자에게 제공하여 관람 및 전시에 관련된 정보를 빠르게 제공하여 많은 사용자가 전시회를 관람을 효과적으로 제공할 수 있도록 하였다.[8]



〔그림 3〕 실내 위치 서비스를 활용한 정보제공

3.2.2. 해외 비콘 활용 동향

해외에 혁신적인 활용 예는 다양하지만 가장 적극적인 적용 및 개발은 미국 모바일 및 PC제조업체 애플의 사례를 들 수 있다.

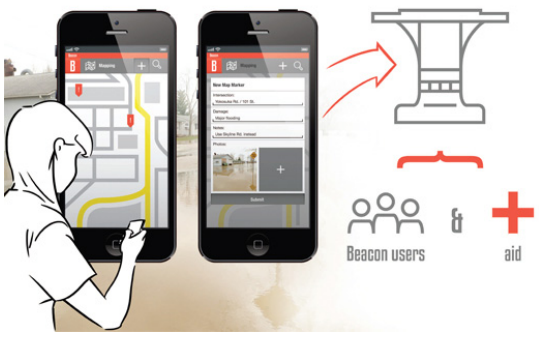
미 프로야구 메이저리그 및 각종 백화점 체인 업체들과의 협력으로 iBeacon을 미국 내 254개 애플스토어에서 iBeacon서비스를 시작하였다. 애플스토어에 설치된 iBeacon 위치에 사용자가 지나가게 되면 사용자의 iPhone 업그레이드 상태, 보상판매 가능 유·무 에 관한 정보를 제공한다.

애플은 iBeacon에 대한 규격을 공개하고 자사의 MFi(Made For iPhone) 프로그램을 통해 관련 디바이스의 인증을 시작하였는데 iBeacon의 경우 지원 대상이 iOS 단말로 한정된다는 점에서 사업 확장 측면에서 한계가 존재하지만, 폐쇄적인 만큼 관련 서비스 품질 관리가 쉽다는 특징이 있다. 또한 결제시스템 기업인 페이팔(PayPal)은 PC의 USB 포트나 전원 콘센트에 삽입하는 방식의 매장용 송수신기 'PayPal Beacon'을 개발 및 운영하고 있다.

PayPal Beacon은 소비자의 스마트폰에 설치된 페이팔 모바일 앱과 블루투스를 통해 정보를 주고받는 역할을 수행한다. 페이팔 모바일 앱이 설치된 스마트폰을 소지한 고객이 매장에 들어오면 PayPal Beacon이 해당 소비자에게 할인 정보나 매장 안내 등의 정보를 제공하거나 페이팔 앱을 통해 물품 대금을 지불하는 등의 활용이 가능하다.[9]

3.3. 기반 기술 - 저전력 블루투스v4.0

비콘은 블루투스 4.0 기반의 근거리 무선통신 장치이다. 블루투스 v4.0은 사용자에게 LTE와의 공존성을 높여 편의성을 상승시키고, 대용량 데이터 전송을 가능하게 할 뿐만 아니라 기존 블루투스에 저전력 요소가 추가됨으로서 상호 연결되는 기기 간 배터리 소모량을 크



〔그림 4〕 사용자에게 다양한 정보제공

Specifications	Bluetooth 1.1	Bluetooth 1.2	Bluetooth 2.0	Bluetooth 2.1 plus EDR (Enhanced Data Rate)	Bluetooth 3.0	Bluetooth 4.0
Voice dialing	Yes	Yes	Yes	Yes	Yes	Yes
Call mute	Yes	Yes	Yes	Yes	Yes	Yes
Last-number redial	Yes	Yes	Yes	Yes	Yes	Yes
Improved Fast transmission speeds		Yes	Yes Yes	Yes Yes	Yes Yes	Yes Yes
Lower power consumption			Yes	Yes	Yes	Yes
Improved pairing (without a PIN)				Yes	Yes	Yes
Greater security		Yes	Yes	Yes	Yes	Yes
Bluetooth Low Energy						Yes
NFC Support			Yes	Yes	Yes	Yes

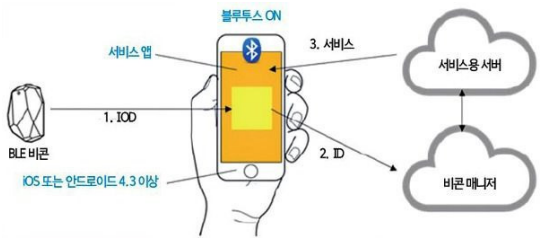
〔그림 5〕 블루투스 버전 별 비교〔10〕

게 감소시켰다.

3.4 비콘 동작원리

비콘 서비스는 스마트폰 내부의 앱을 통해 비콘 기기 신호를 수신해 비콘 전용서버에 질의하면 서버가 해당 정보를 취득하고 앱에 표시하는 순환 구조로 가지고 있다. 비콘 송신기가 주기적으로 ID와 RSSI(Received Signal Strength Indicator)값을 신호로 송신, 스마트폰 사용자가 송신 신호의 도달 거리 내로 진입하면 스마트폰 앱이 이를 인식해 클라우드 서버로 사용자 정보를 전달하고, 전용 서버에서 사용자의 개별 정보를 활용하여 관련된 콘텐츠를 사용자에게 송신하고 스마트폰을 통해 사용자가 인식하는 방식을 활용하는 것이다.

즉, 중간 서버가 존재하는 것으로 비콘 기기 자체는



〔그림 6〕 BLE 기반 비콘 동작 흐름

신호를 송신하는 역할만 하는 것이고 비콘 전용서버는 비콘 범위내 사용자의 개별정보를 수신받고 콘텐츠 내용을 송신 하는 것이다.[9]

3.5 비콘의 취약점

비콘은 다양한 컴퓨팅 환경에서 기반 기술로 활용되지만 대부분 블루투스 4.0을 기반 방식으로 적용 하고 있다. 가장 주목할 부분은 저전력이라는 장점을 가진 블루투스 4.0은 장시간 작동해야하는 비콘 기기에 적합한 기능인데 반해 생각해보면 장시간 취약점에 노출되어 있다고 생각할 수 있다. 또한 일정한 주파수를 사용하는 블루투스의 취약점을 가지고 있지만 다른 같은 대역의 주파수 사용기기와 충돌을 피하기 위하여 1초당 1,600번의 주파수를 바꿔가며 전송하는 주파수 호핑(hopping) 기술을 적용하며 안전성을 어느 정도 확보했지만 지속적인 주파수 교란 공격을 가한다면 해킹도 가능하다.

비콘이 일방향 통신이기 때문에 내재적인 보안취약점이 없다고 판단할 수 있으나 이는 잘못된 판단이다. 비콘의 대 사용자에 대한 일방향 주파수 송신은 맞지만 그 송신을 통해 전용콘텐츠 서버로, 비콘 매니저로 개별정보가 송·수신된다. 이 과정에서 제공되는 정보가 왜곡될 수 있다는 것이다. 즉 무결성 위배가 가능하다.

또한 지속적으로 주파수를 송·수신 하기 때문에 해당 어플리케이션을 통한 지속적인 개별정보를 송·수신 함으로써 사용자의 위치도 노출되어 개인 사생활도 침해할 가능성이 있다. 위의 비콘의 동작원리에 의해 비콘의 현재 보안 기술도 안전하다고 판단할 수 없다.

위의 BLE기반의 비콘 동작 원리를 통해 확인할 수 있는 취약점은 다양하지만 대표적으로 다음과 같은 이슈가 있다.

비콘 기기에 관련된 서비스 인프라는 아직 초기단계라고 볼 수 있다. 비콘 서비스의 동작 방식에 따른 예상되는 취약점은 다음과 같다.

- 네트워크 상에서 MAC주소, IP주소 등 네트워크 통신과 관련된 정보를 변경하여 통신 흐름을 왜곡시키는 스푸핑(Spoofing)
- 원본 시스템에서 부과한 세션 정보 또는 개별 정보를 복사하여 기존에 연결 되어있던 대사물의 정보를 복

사하고 해당 개별 정보를 활용하여 원래 대상처럼 속여서 정보를 빼내는 클로닝(Cloning)

- 블루투스 기반으로 하는 비콘은 블루투스 자체로 2.45GHZ 내에 많은 채널로 나누어져 있지만 지속적인 전파 간섭 및 교란 신호 공격으로 서비스 오동작에 문제를 발생시키는 블루투스 서비스 거부 공격(BDOS)

하지만 가장 취약한 점은 비콘 서비스 관련 어플리케이션에 있다. 많은 기업 및 산업들이 모바일 실시간 홍보 서비스 또는 정보 제공 서비스로 비콘을 활용할 것으로 예상되는데 이러한 서비스가 확장되면 매우 취약한 부분으로 작용될 수 있다.

비콘은 여러 가지 기능이 있지만 근접위치 정보를 통해 해당 서비스가 활성화 되면 실내에서 사용자의 이동 정보를 오차범위 5cm 이내로 측정이 가능하다. 이는 사용자의 모바일이 취약한 비콘 기기 또는 공격자의 기기 근처를 지나가게 되면 사용자가 소지하는 모바일 내 비콘 서비스 어플리케이션에 신호를 보내면 사용자는 자동적으로 무분별하게 취약한 비콘 서버 또는 공격자의 비콘 서버에서 보내는 데이터를 받을 것이다.

이 때 송·수신 콘텐츠에 악성코드를 삽입하는 공격원리를 활용하여 트로이 목마, 피싱 공격을 활용하여 이벤트 당첨 문자 등으로 위장하고 악성 코드가 있는 공격자의 웹사이트URL을 걸어놓거나 악성 앱을 다운받게 만든다. 이를 통해 사용자 기기에 악성코드 전송이 가능하다.

블루투스 4.0 기반의 비콘 기술은 기존 블루투스의 취약점일부도 존재한다. 또한 비콘의 동작 원리와 활용도에 따라서 위의 내용보다 더 많은 취약점이 발생할 수 있는 것이다. 향후 무선 결제 등에 선두주자로 적용될 기술이라고 전망한다면 확실한 기밀성과 무결성이 보장되어야 한다.

비콘이 적용될 새로운 IoT산업 분야 중 가장 큰 시장을 형성할 것으로 예상되는 제품은 스마트 자동차 이다. 현재 일정지역에 차량이 접근하게 되면 해당 지역 및 도로 교통에 관한 정보를 수신하고, 그에 따라 차량에 관련 정보를 송·수신하게 된다. 유용한 콘텐츠제공이라는 부분에서는 좋은 기능이지만 표적형 공격에도 활용될 수 있다.

가령 악성 콘텐츠를 전송하는 비콘을 제작한 공격자들이 유명인사 혹은 공인의 이동경로를 사전에 파악하고 악성 비콘을 이동 경로에 사전 설치 한 후 정상적인 콘텐츠를 제공하는 것처럼 위장하여 악성 코드 전공이나 차량 내 통신기기에 악영향을 미치는 동작도 가능하다.

특히 스마트 자동차 간 정보 제공 역시 비콘을 활용하게 되고, 악성코드에 감염된 스마트 자동차와 정보를 상호간 송·수신하는 차량 역시 악성코드 감염의 위험이 높아진다.

Ⅳ. 대응 방안

4.1. 컴플라이언스 및 관리적 측면의 대응

비콘을 활용하는 서비스 및 실내 측위 기술을 활용 시 사용 주체는 비콘 활용 안에 대한 계획을 수립해야 한다. 설치 위치, 설치 개수, 송신하는 콘텐츠 종류, 설치 위치별 비콘 동작 시간, 주파수 설정 및 활용되는 장소, 공간의 크기를 고려하여 비콘 활용 계획을 수립하고 이를 통해 비콘이 사용되는 목표에 대한 동작만 수행하도록 해야 한다.

또한 제도적으로 비콘 정보 송신 간 해당 콘텐츠의 내용표시를 하도록 하는 규정을 통해 사용자가 사전에 알 수 있도록 해야하며, 거짓 내용 및 불필요 내용을 표시할 경우 불법 행위로 간주 할 수 있도록 제도적 마련이 필요하다.

4.2. 어플리케이션 개선을 통한 대응

실내 측위 및 모바일 별 이동 경로에 따른 정보수집에 대해서는 사용자가 비콘 동작 범위로 이동하는 경우 정보수집에 대한 문구 및 동의 여부에 대해서 사용자 측의 선택이 가능하도록 어플리케이션 개발을 해야 한다. 이는 해당 모바일 운영체제 및 비콘을 수신하는 어플리케이션에서 비콘 으로부터 정보를 수신하기 전에 alert banner를 통해 수신 여부를 제어할 수 있도록 해야 하고, 콘텐츠 정보 제공 받은 후 해당 프로그램에서는 제공 받은 콘텐츠 임시파일을 삭제할 수 있도록 해야하며, 저용량으로 정보를 제공한 비콘의 고유번호, 정보 제공 받은 시점 등을 로그기록으로 남겨 향 후 사고 발생시 불법적인 비콘 활용에 대한 추적이 가능하도록 해야 한다.

4.3 물리적 측면의 대응

기존에 활용되던 블루투스 4.0보다 상위 버전을 활용함으로서 일정 부분 대응할 수 있다. 4.1 및 4.2버전은 기존 비콘에서 활용된 4.0버전의 취약점과 성능을 일부 개선하였다. 하지만 블루투스를 기반으로 둔 비콘은 블루투스가 본질적으로 가지고 있는 취약점을 개선하지 않으면 안된다.

블루투스의 무선통신 인증 방식에 활용되는 AES 알고리즘 뿐 만 아니라 다른 우수한 암호 알고리즘을 활용하는 것이다. 예를 들면 국산 암호 알고리즘 중에 하나인 저전력, 경량화 환경에 초점을 둔 HIGHT 알고리즘의 활용도 하나의 대응 방안이 될 수 있다.

또한 비콘과 불특정 다수의 사용자 간의 주파수 연결 시 외부 주파수의 방해로 주파수 내 채널에 영향이 있을 시 외부 주파수를 차단하거나, 잠시 사용자와의 연결을 끊고 자동적으로 재연결하는 기능을 개발함으로서 기존 스푸핑 및 스니핑 취약점에 대한 물리적 대응이 가능하다.

Ⅴ. 결 론

본 연구를 통해 블루투스 4.0을 기반으로 한 비콘 활용을 통해 예상되는 취약점을 알아보았다. 비콘 활용 분야는 마케팅, 스마트 자동차, 드론, 모바일 등의 산업 전반에 걸쳐 매우 광범위 하다. 향 후 더 많은 분야로 비콘은 활용될 것이며, 단순한 콘텐츠 송신기로서의 역할 그 이상으로 활용될 것으로 판단된다. 하지만 비콘 취약점이 개선되지 않는 이상 사용자들의 소중한 정보자산은 비콘의 활용범위가 늘어날수록 위험도 커질 것이며, 비콘과 관련된 기기 사용에 이상이 생길 것이다.

본 논문은 블루투스 기반의 비콘이 활용됨으로써 예상되는 취약점을 연구하였다. 비콘이 동작하는 방식과 활용 분야 마다 발생할 수 있는 공통적인 예상 취약점을 블루투스 거부공격(BDOS), MITM공격, Sniffing 및 Spoofing으로 예상·분석하고 그에 대한 대응 방안을 컴플라이언스 및 관리적 측면, 어플리케이션을 통한 측면, 물리적 측면으로 나누어 제시하였다.

향후 필요 연구로는 비콘이 활용되는 분야를 세부적으로 나누고, 분야 별 비콘을 통한 공격 기법 및 기능적인 대응 방안과 비콘 개발 시 적용해야하는 보안 모듈 개발 제안을 통해 기밀성·무결성·가용성을 한 단계 상승시킬 수 있는 연구가 필요하다.

참 고 문 헌

[1] Riku Mettala, “Bluetooth Protocol Architecture Version 1.0”, Bluetooth SIG(Bluetooth Special), Aug 1999.

[2] karen Scarfone, John Padgette, "Guide to Bluetooth Security", Nist Secial Publication 800-121, Sem 2008.

[3] 강동호, 백광호, 김기영, “블루투스 보안 기술”, 정보통신연구진흥원, 2009년 1월.

[4] Nate Be-Nazir Ibn Minar, Mohammed Tarique, "BLUETOOTH SECURITY THREATS AND SOLUTIONS : A SURVEY", International Journal of Distributed and Parallel Systems(IJDPS), January 2012.

[5] DATA NET, "BLE 기반 근거리 데이터 통신 기술로 주목", http://www.datanet.co.kr/news/articleView.html?idxno=78060.

[6] usiness Line - BitHub, "비콘(Beacon)이 주목 받는 까닭은?", http://www.bithub.co.kr/n_news/news/view.html?page_code=photo&photo_theme=&no=6089&PHPSESSID=c4b9ac2a187cb9e8994f1bb966923b89.

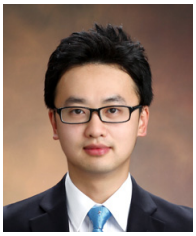
[7] 이정아, "비콘 서비스 부상과 새로운 비즈니스 확산",한국정보화진흥원, 2014년 12월.

[8] 남궁현, "블루투스 저에너지 비콘을 활용한 측정 신호 분석 및 비교 시스템", 한남대학교 학위논문, 2015년 2월.

[9] 방송통신진흥본부 미디어산업진흥부, "비콘, 위치기반 서비스의 핵심 인프라로 급부상", 한국방송통신전파진흥원, 동향과 전망 : 방송·통신·전파 통권 제73호, 2014년 04월.

[10] Smart Fone Arena, "Samsung Patent Dispute continues", http://smartfonearena.com/samsung-patent-dispute-continues/

〈저 자 소 개〉



김 승 일 (Kim Seung IL)
학생회원

2015년 2월 : CSLAC 웹 진단 컨설턴트 근무
2015년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 웹 보안, 개발 보안, 침투 테스트, 악성코드 분석

지 선 학 (Seon-Hak Ji)
학생회원

2015년 2월 : 강원대학교 정보통신공학과 졸업
2015년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 모바일보안, S/W보안, 악성코드

이 재 우 (Jae-Woo Lee)

동국대학교 국제정보대학원 석좌교수(현)
한국포렌식조사전문가협회 회장(현)
ISC2 Fellow, Asia Board 의장(현)
한국 CSO 협회 자문위원장(현)
한국정보보호진흥원 초대 원장