논문 리뷰
저전력 블루투스(BLE) 비콘 보안 취약점 연구

발표자: 양유진

링크: https://youtu.be/iBoqGSRB5WE

1. 서론

- ICT(Information Communications Technologies) 환경 폭발적 성장 → 여러 분야에 IoT가 다양한 용도로 활용됨
- 블루투스 무선 통신 기술이 무선 통신 사업에 활용되고 있는 중요한 기술 中 하나임.
- 블루투스 기반인 '비콘'은 기존의 블루투스 통신 기술 자체의 보안 취약점을 가짐.

2. 블루투스(Bluetooth) 기술 2.1 블루투스 프로토콜

1. Host Controller Interface

- Baseband, Linkmanager, Hardware 등을 접근·제어하기 위한 표준화된 인터페이스
- 인터페이스 방법 통일 → 하드웨어에 따라 애플리케이션 따로 제작할 필요X

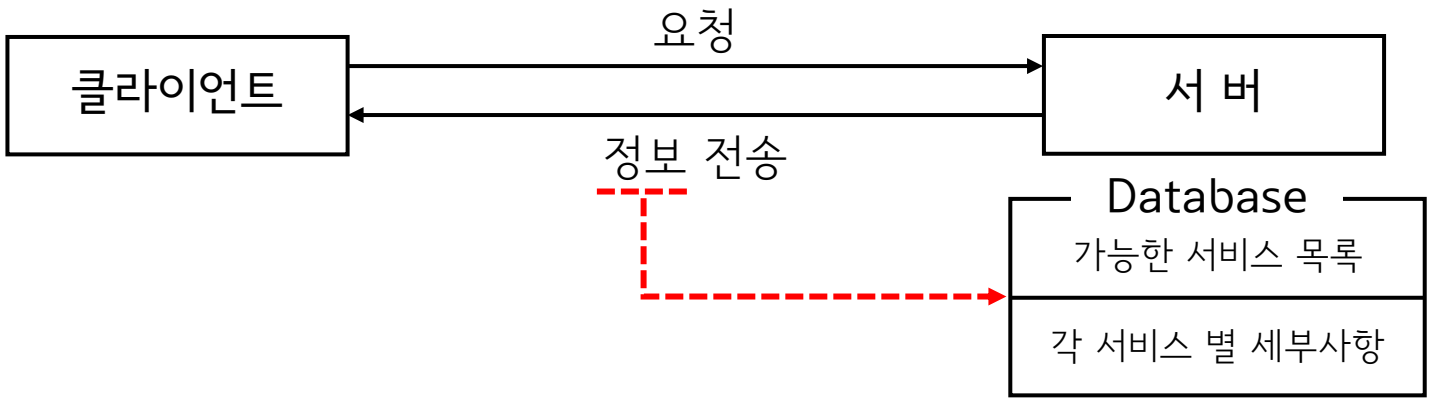
2. L2CAP

- 상위 계층 프로토콜-하위 계층 프로토콜(HCI, Baseband) 중재・조정함
- 프로토콜 멀티 플랙싱, 분할, 재조합

2. 블루투스(Bluetooth) 기술 2.1 블루투스 프로토콜

3. SDP

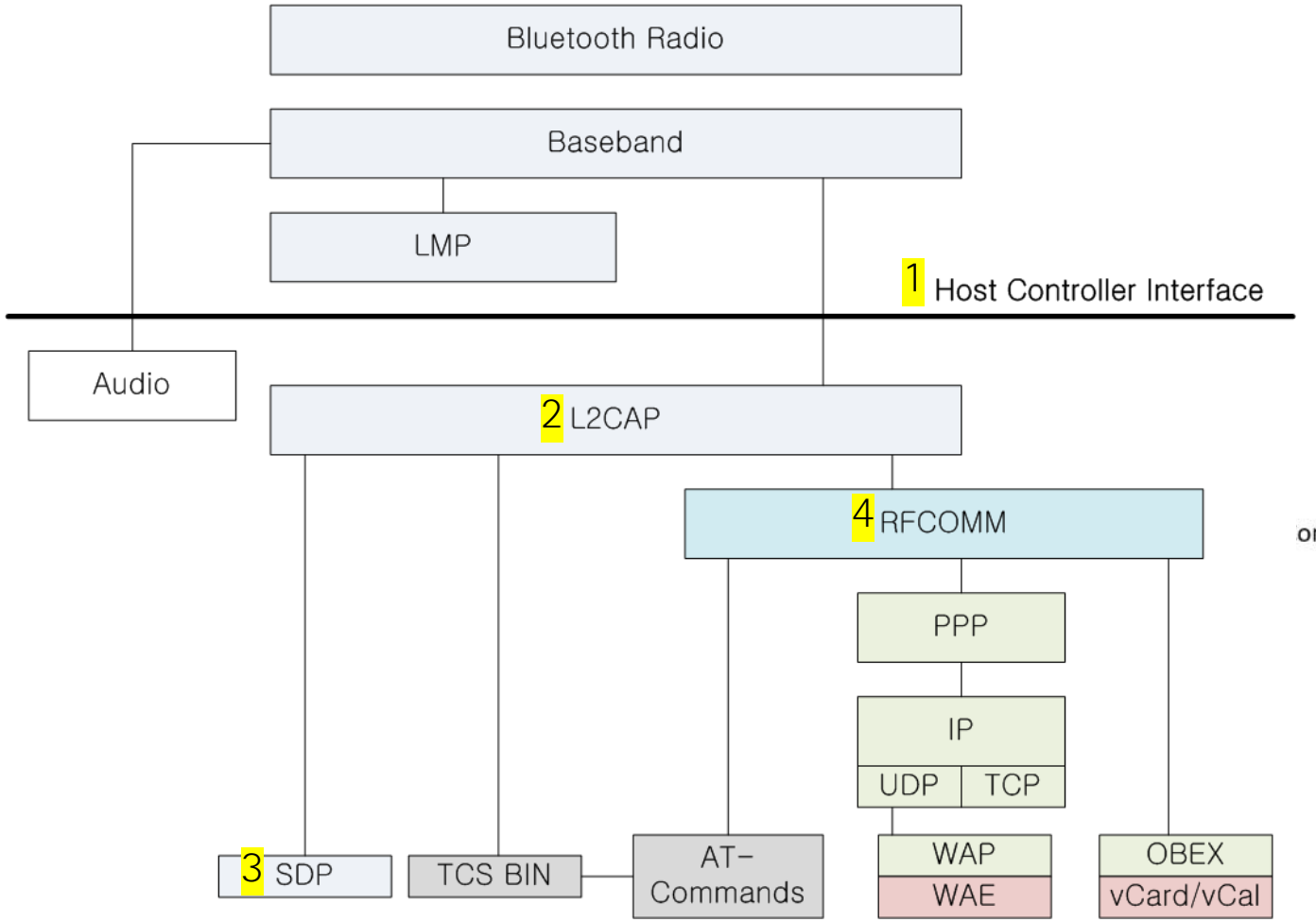
- 연결된 블루투스 장치에서 정보(가능한 서비스, 서비스 별 특징) 교환하기 위한 프로토콜
- 서버・클라이언트 구조



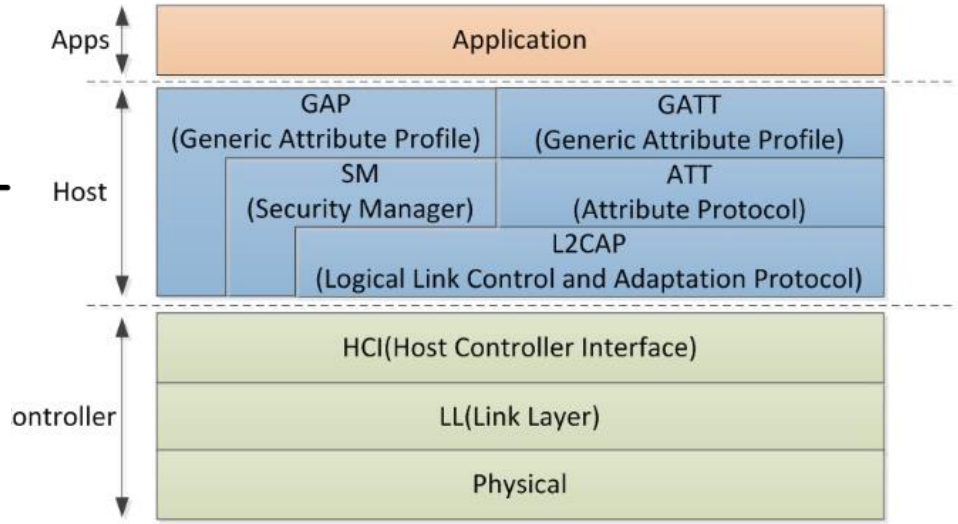
4. RFCOMM

- RS-232 시리얼 포트를 에뮬레이션하는 역할함
- 동시에 60개 포트를 열 수 있는 다중 에뮬레이션 지원함

2. 블루투스(Bluetooth) 기술 2.1 블루투스 프로토콜



(그림 1) 블루투스 프로토콜 스택



출처: https://neosla.tistory.com/49

2. 블루투스(Bluetooth) 기술 2.2 블루투스 보안 매니저

2.2.1 블루투스 보안 레벨

1) 장치 신뢰 레벨 관리

- 신뢰 장치(Trusted Device): 인증된 장치 + 링크키 저장 + 디바이스 DB에 'Trusted'로 정의된 장치
- 비신뢰 장치(Untrusted Device): 인증된 장치 + 링크키 저장 + 디바이스 DB에 'Trusted'로 정의되지 **않은** 장치
- 알려지지 않은 장치(Unknown Device): 보안 관련 정보가 없는 장치

2) 블루투스 보안 모드

- Security Mode1: 보안기능 제공X / 블루투스 장치는 Promiscuous 상태 / 별도의 보안기능 없이 연결·접근 가능
- Security Mode2: Service Level 보안 모드 / LMP 링크 연결 후~L2CAP 채널 연결 전에 동작함 / 보안 매니저가 특정 장치·서비스 접근 허용 여부 결정
- Security Mode3: Link Level 보안 모드 / 물리적 링크가 완전히 설정되기 전에 동작함 / 모든 장치간 연결에 인증 ·암호 적용
- Security Mode4: Service Level 보안 모드 / Mode2보다 보안 기능 강화 & 페어링 단순화

2. 블루투스(Bluetooth) 기술 2.2 블루투스 보안 매니저

블루투스는 Link Level에서 보안 매니저를 통해 보안 관련 처리를 담당함

[주요 특징]

- 장치/서비스 관련 보안 정보 관리
- 프로토콜·응용 프로그램 보안 관련 질의응답
- 인증 및 암호화 수행

2.2.2 인증

인증 절차는 요구자(Claimant), 검증자(Verifier)로 구성된 Challenge-Response 형태임

1) 요구자가 검증자에게 자신을 증명하도록 시도함
2) 검증자는 링크키를 이용하여 요구자의 증명을 검증함

2.2.3 기밀성

데이터 암호화 기능 제공 → 상호간 주고 받는 데이터 도청 방지

2. 블루투스(Bluetooth) 기술 2.3 블루투스 취약점

1) Bluetooth Scanner

- 블루투스 단말기 취약점 공격을 위해 주변지역의 블루투스 지원 단말기를 스캔하는 공격
- 지원 서비스 확인 단계(단말기 프로파일 탐색)가 우선적으로 이뤄짐
- 검색 기능 제공 → 발견된 장치에 대한 정보 추출

2) Bluesnarfing

- 펌웨어 취약점 이용 → 장치내 저장된 데이터에 대한 접근 허용하는 공격

3) Bluejacking

- 블루투스 지원 단말기에 스팸, 피싱 공격을 시도하는 파일·메시지 전송하는 공격

4) Bluebugging

- 펌웨어 취약점 이용 → 장치 접근 권한 획득하는 공격

5) Denial of Service

- 블루투스 지원 단말기에 지속적으로 데이터 전송 → 배터리 소모or단말기 재부팅 → 정상적인 사용 방해하는 공격

3. 비콘(Beacon) 기술 3.1 블루투스 v4.0기반 비콘 특징

1) 소량의 패킷 (168bits=21bytes)
2) 주기적 신호
3) 페어링 불필요
4) 저전력 (3V 코인전지, 200~300ms 주기기준, 약 2년)
5) 도달거리: 최대 50m, 안정권 20~30m
6) Ios7, Android 4.3이상 지원
7) 블루투스 켜져 있어야 신호 수신O
8) 저비용
9) 소형, 설치보단 **부착**의 개념
10) UUID + Major + Minor + RSSI

보내는 신호는 **비콘 송신기 ID**, RSSI만 가짐

- UUID(Universally Unique Identifier, 범용 고유 식별자): 네트워크 상에서 고유성이 보장되는 ID를 만들기 위한 표준 규약
- Major: 동일한 UUID를 가진 비콘을 구분할 때 사용됨
- Minor: 동일한 UUID, Major를 가진 비콘을 구분할 때 사용됨

위치판별(지역, 세부 장소)

- RSSI(Received Signal Strength Indicator): 수신되는 신호 강도

3. 비콘(Beacon) 기술 3.2 국내외 비콘 활용 동향

3.2.1 국내 비콘 활용 동향

1) BC카드, 롯데카드

- 관광객, 멤버십 대상의 비콘 서비스 실시
- 국내 관광서비스질 향상과 외국 관광객의 국내 관광 서비스 만족도 향상에 이바지함.

2) 이동통신사(LGU+, SKTelecom)

- 실내 위치 정보 기반하여 모바일 앱으로 실시간 경기 정보, 가이드 서비스 제공

3.2.2 국외 비콘 활용 동향

1) iBeacon (Apple)

- 사용자의 iPhone 업그레이드 상태, 보상판매 가능 유·무 에 관한 정보 제공

2) PayPal Beacon (PayPal)

- 앱을 통해 소비자에게 정보(할인 정보, 매장 안내 등) 제공하거나 물품 대금 지불 가능

3. 비콘(Beacon) 기술 3.3 기반 기술 - 저전력 블루투스v4.0

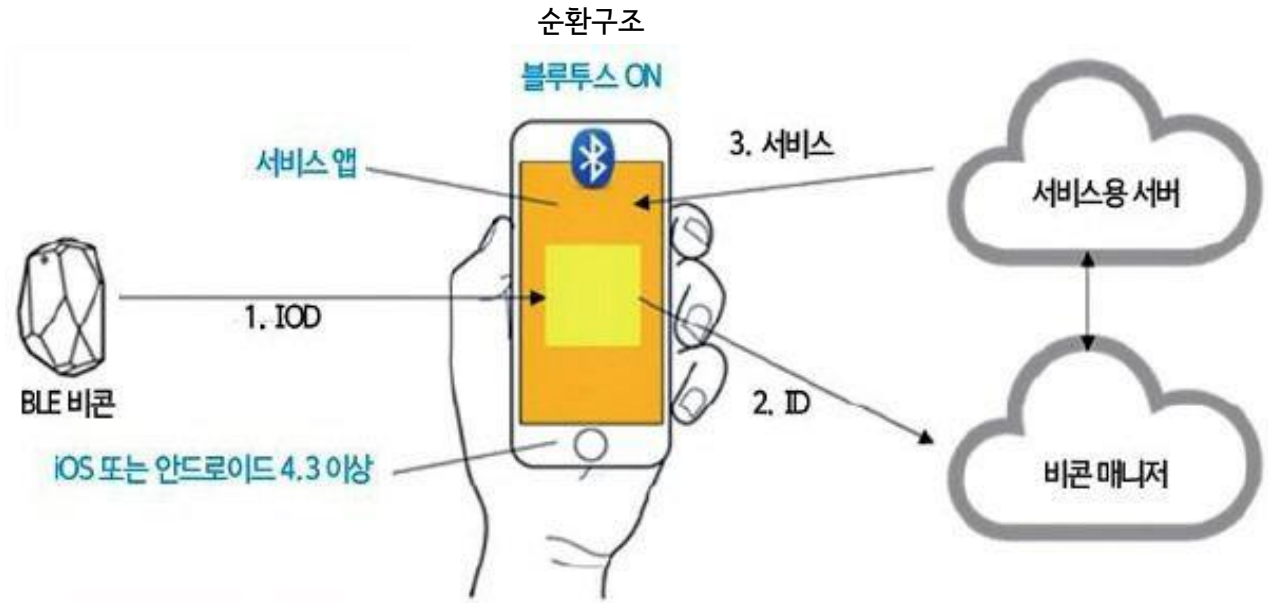
- 블루투스 v4.0은 LTE와의 공존성이 높음 → 편의성 상승, 대용량 데이터 전송 가능함
- 저전력 요소 추가 → 기기간 배터리 소모량 크게 감소함

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		Yes	Yes	Yes	Yes	Yes
Fast transmission speeds			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

3. 비콘(Beacon) 기술 3.4 비콘 동작원리

1) 비콘 기기가 주기적으로 신호(ID & RSSI) 수신함
2) 스마트폰 앱이 이 신호를 인식하면 클라우드 서버로 사용자 정보 전달함
3) 전용 서버에서 사용자의 개별 정보를 활용하여 관련된 컨텐츠를 앱에 전송
4) 사용자는 어플을 통해 인식할 수 있음



(그림 6) BLE 기반 비콘 동작 흐름

3. 비콘(Beacon) 기술 3.5 비콘의 취약점

- 장시간 작동 → 장시간 취약점 노출
- 지속적인 주파수 교란 공격 → 해킹 가능
- **무결성 위배:** 전용 콘텐츠 서버, 비콘 매니저로 개별 정보 송수신 될 때 제공되는 정보 왜곡 가능성 있음
- 지속적 주파수 송수신 → 지속적 개별정보 송수신 → 사용자 위치 노출 → 개인 사생활 침해 우려

<비콘 서비스 동작원리>

- **스푸핑(spoofing):** 네트워크 상에서 통신 관련 정보(MAC주소, IP주소 등) 변경 → 통신 흐름 왜곡
- **클로닝(cloning):** 원본 시스템에서 부과한 세션 정보/개별정보 복사 → 원래 대상인척 속여 정보 탈취
- **블루투스 서비스 거부 공격(BDOS):** 지속적인 전파간섭/교란 신호 공격 → 서비스 동작에 문제 발생

<비콘 서비스 관련 어플리케이션>

- 사용자가 자동적으로 취약한 비콘 서버 또는 공격자의 비콘 서버에서 보내는 데이터를 받을 경우, 사용자 기기에 악성코드 전송 가능해짐. (악성코드 삽입 공격)
- 피해자의 이동경로를 사전에 파악하고 악성 비콘을 이동 경로에 사전 설치한 경우 스마트카 내 통신기기에 악영향 미치는 동작 가능함.

4. 대응 방안 4.1 컴플라이언스 및 관리적 측면의 대응

- 사용 주체는 비콘을 활용하는 서비스, 실내 측위 기술 활용 시, 비콘 활용에 대한 계획을 수립해야 함.
- 수립한 계획을 통해 비콘이 사용되는 목표에 대한 동작만 수행하도록 해야 함.
- 비콘 정보를 전달할 때, 해당 콘텐츠의 내용을 표시 하도록 규정 → 사용자가 사전에 알 수 있게 해야 함.
- 거짓/불필요한 내용을 표시할 경우 불법 행위로 간주할 수 있도록 제도적 마련이 필요함.

4. 대응 방안 4.2 어플리케이션 개선을 통한 대응

- alert banner를 통해 비콘 수신 여부 제어할 수 있게 해야 함.
- 콘텐츠 제공 받은 후 콘텐츠 임시파일 삭제할 수 있게 해야 함.
- 저용량 정보를 제공한 비콘의 고유번호, 정보 제공 받은 시점을 로그기록으로 남김
  → 사고 발생 시, 불법적 비콘 활용 추적 가능케 해야 함.

4. 대응 방안 4.3 물리적 측면의 대응

- 블루투스 v4.0 상위 버전 활용 → 일부 대응 가능
- 블루투스 무선통신 인증 방식에 우수한 암호 알고리즘 적용
- 외부 주파수 방해로 주파수 내 채널에 영향 있을 때,
  외부 주파수 차단 & 잠깐 연결 끊고 자동 재 연결해주는 기능 개발
  → 스푸핑, 스니핑 취약점에 물리적으로 대응 가능함.

5. 결론

- 더 많은 분야에 활용될 것으로 예상되는 비콘의 취약점 개선이 필요하다.

- 향후, 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 상승시킬 수 있는 연구가 필요하다.

감사합니다