BlueTooth 해킹

201819170 우자영

BlueTooth의 개념 & 프로토콜 형식

BlueTooth의 개념 & 프로토콜 형식

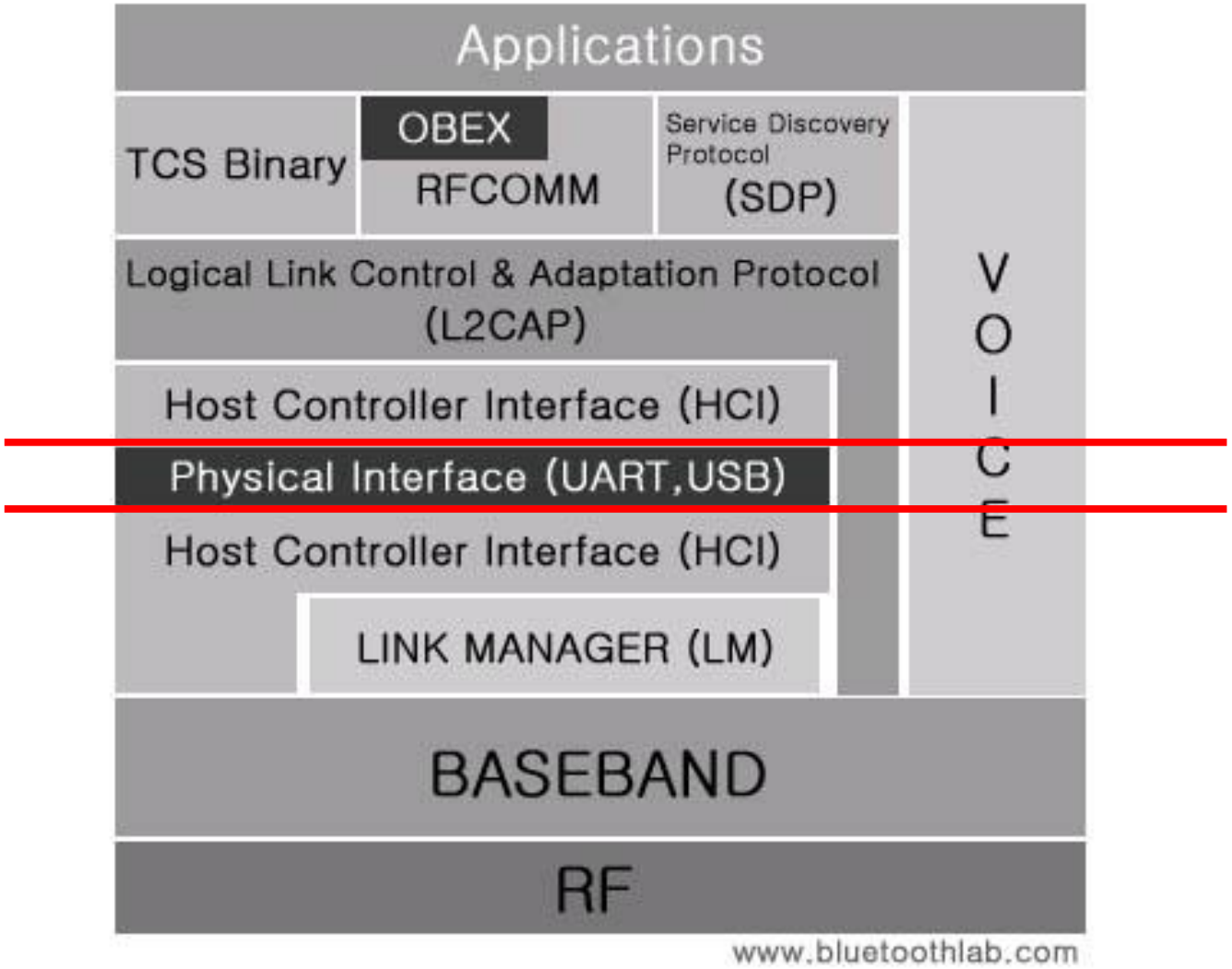
Bluetooth란?

- 근거리 무선 네트워크 WPAN(Wireless Personal Area Network)의 한 표준
- 공통 대역, ISM 주파수 대역(사업, 과학, 의료용으로 할당된 주파수 대역)을 사용
- 2.4 ~ 2.48GHz 범위 내 79개의 채널 이용
- 주파수 호핑 방식(Frequency Hopping FH) : 많은 채널을 특정 패턴에 맞추어 빠르게 이동하면서, 데이터를 조금씩 전송하는 기법

용어
Inquiry : 스캔과 유사, 응답으로 MAC과 이름이 담김
Paging : Connection 상태가 되기 위해 실제 연결 되는 단계

BlueTooth의 개념 & 프로토콜 형식

Bluetooth 프로토콜 스택



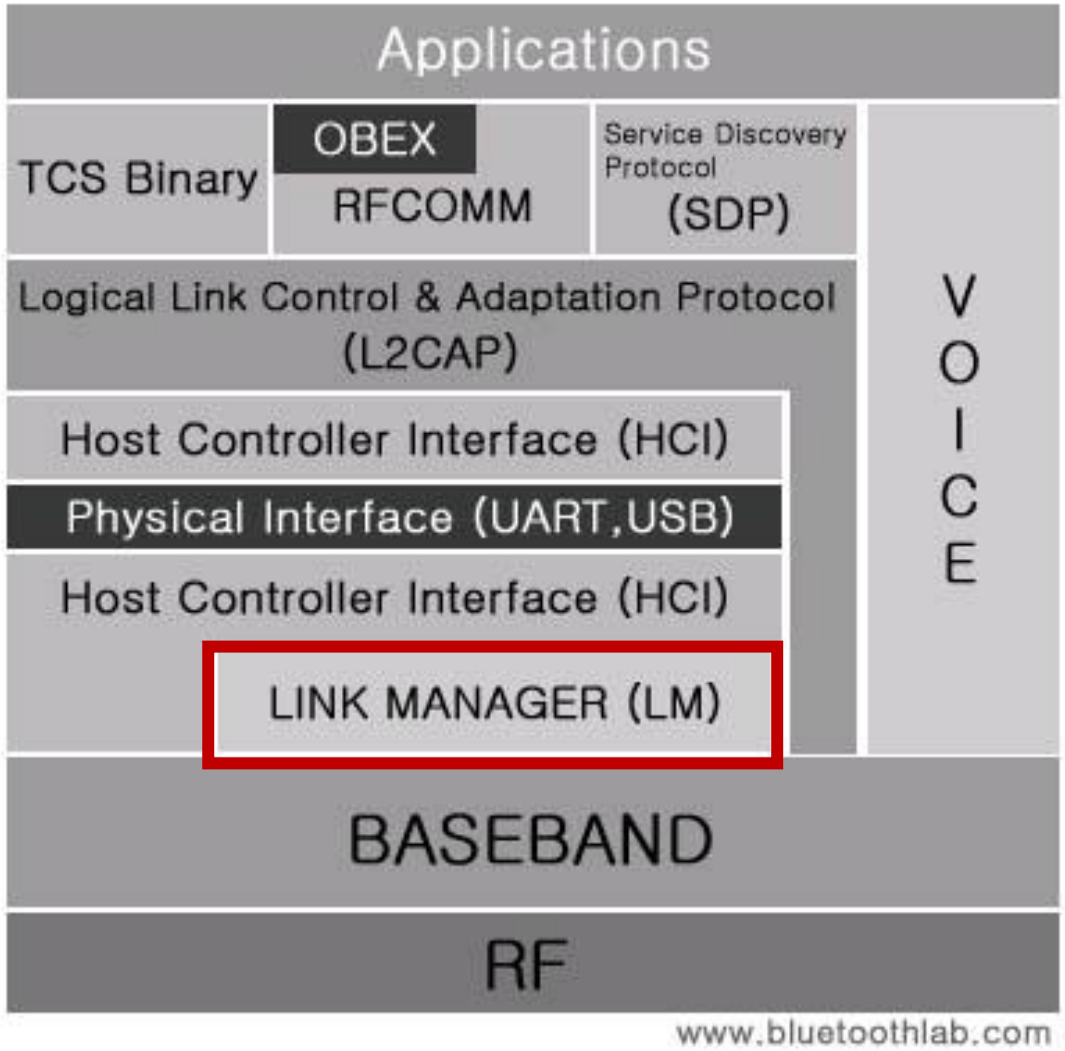
← Host Protocol
(PC, 핸드폰, 마이크로 프로세서 등)
- 블루투스 모듈 제어, 어플리케이션 수행
- 어플리케이션의 종류나 Profile에 따라 달라짐

Profile : 사용할 프로토콜의 종류, 구조, 사용방법을 의미

← Host Controller Protocol
(블루투스 모듈)
- 펌웨어 형태로 모듈 내부에 포함

BlueTooth의 개념 & 프로토콜 형식

Bluetooth 프로토콜 - LM (Link Manager)



- Link 설정
- 보안 설정

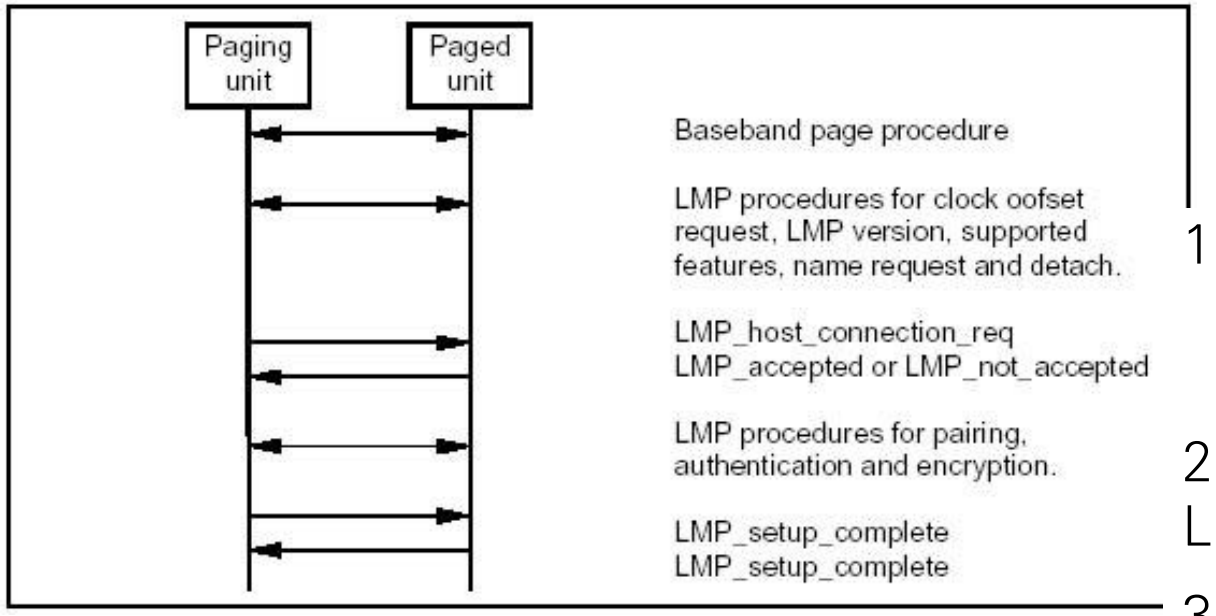
인증을 위한 Link Key 교환, Paring 등을 수행, 암호화

- 제어 (클럭 및 슬롯 관리)
- LM 사이에서 송수신 되는 LMP 메시지 관리
- LMP PDU 교환

LMP : Link Manager Protocol
PDU : Protocol Data Unit

BlueTooth의 개념 & 프로토콜 형식

Bluetooth 프로토콜 - LM (Link Manager)

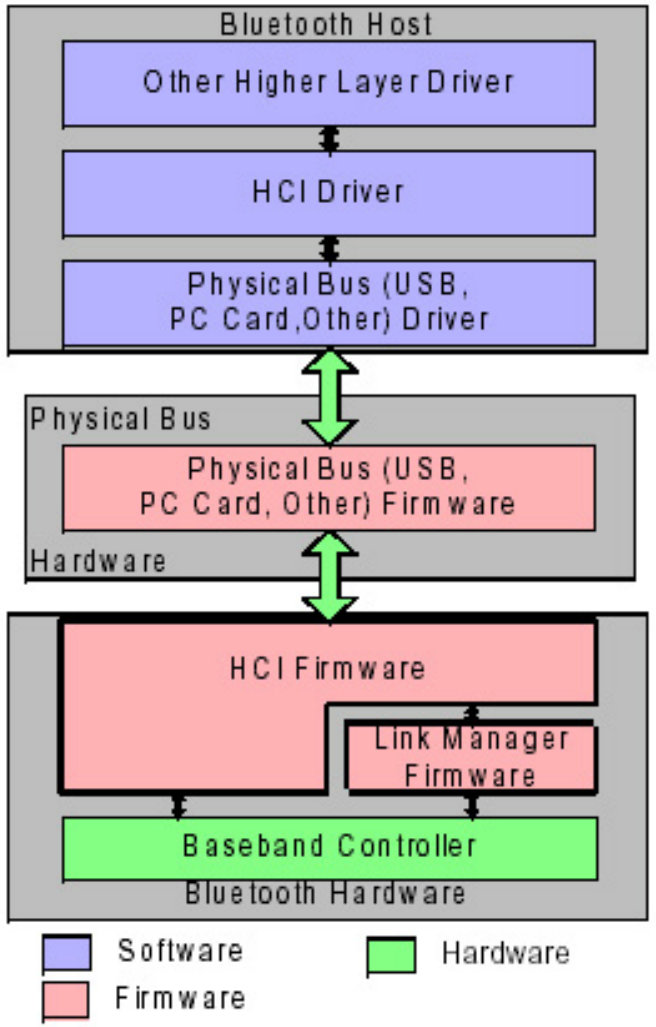


1. 두 장치가 각각 page와 page scan 상태가 된 후, Clock Offset, LMP 버전, 이름 등의 정보를 LMP PDU를 통해 주고 받는다.
2. LMP_host_connection_req 요청과 LMP_accepted or LMP_not_accepted 응답 교환
3. 페어링, 인증, 암호화 등 보안 관련 LMP PDU 교환
4. 완료

LMP : Link Manager Protocol
PDU : Protocol Data Unit

BlueTooth의 개념 & 프로토콜 형식

Bluetooth 프로토콜 - HCI (Host Controller Interface)

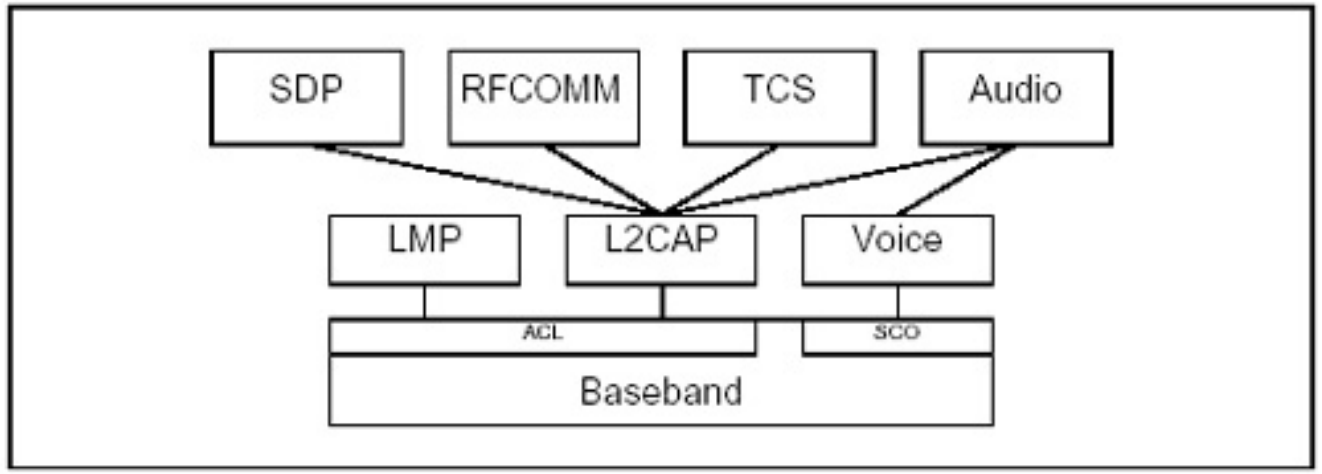


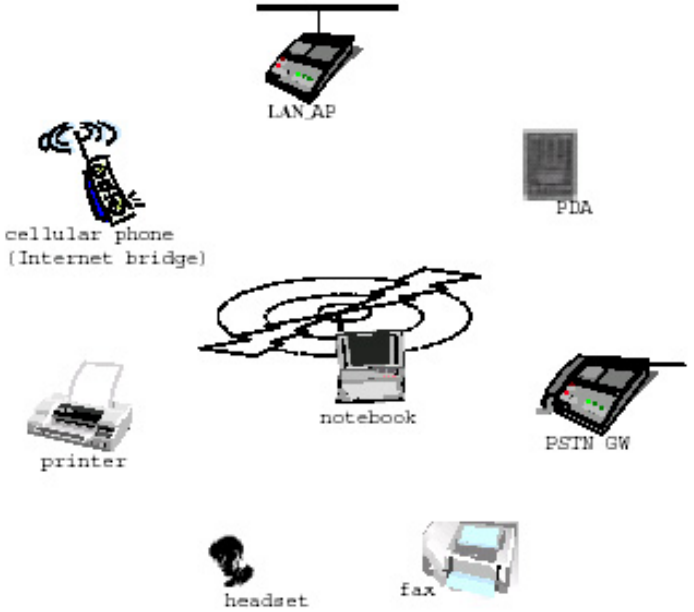
<그림 3> HCI와 하위 계층 프로토콜의 구조

- Bluetooth chip과 host 사이 전송 인터페이스
- 호스트 컨트롤러와 하드웨어 접근 제어
- 호스트, 호스트 컨트롤러 사이 Physical Bus로 통신
- 블루투스 Inquiry, Paging, Connection 등의 링크설정
- 인증, 암호화, 링크 키 등의 보안 및 Connection 상태 설정 실행 가능

BlueTooth의 개념 & 프로토콜 형식

Bluetooth 프로토콜 - L2CAP (Link Control and Adaptation Protocol) & SDP (Service Discovery Protocol)





- L2CAP
상위 계층 (SDP, RFCOMM 등)과 HCI +
하위 계층 (Baseband, LM) 사이 중재 및 조정

- SDP
연결된 블루투스 디바이스에서 가능한 서비스가
무엇인지, 해당 서비스의 특징 교환

BlueTooth 공격 방식

BlueTooth 공격 방식

BluePrinting

블루투스 공격 장치를 검색하는 활동
– 블루투스의 SDP로 공격 가능한 장치 종류를 검색하고 모델을 확인한다.

hcitool & hciconfig
- HCI로 BT MAC 주소, BT 환경 확인

```
┌──(root💀kali)-[~]
└─# hcitool scan
Scanning ...
        FC:[redacted]        Infinity CLUBZ MINI
        94:[redacted]        자영이꺼
        B8:[redacted]        iPhone

┌──(root💀kali)-[~]
└─# hcitool inq
Inquiring ...
        FC:[redacted]        clock offset: 0×0000    class: 0×260404
        94:[redacted]        clock offset: 0×0000    class: 0×240418
        B8:[redacted]        clock offset: 0×0000    class: 0×7a020c
```

sdptool
- SDP(가능한 서비스 확인 프로토콜) 쿼리 수행 도구

```
┌──(root💀kali)-[~]
└─# sdptool browse 94:16:25:2E:3D:0C
Browsing 94:16:25:2E:3D:0C ...
```

btscanner
- 페어링 없이 BT 장치의 많은 정보를 추출하는 도구

```
RSSI:    +0   LQ:  000    TXPWR:  Cur   +0
Address:       F0:6B:CA:32:B5:10
Found by:      00:1A:7D:DA:71:13
OUI owner:     Samsung Electronics Co.,Ltd
First seen:    2022/03/09 08:33:44
Last seen:     2022/03/09 08:33:55
Name:          Galaxy S4
Vulnerable to:
Clk off:       0×0000
Class:         0×5a020c
               Phone/Smart phone
Services:      Networking,Capturing,Object Transfer,Telephony
```

BlueTooth 공격 방식

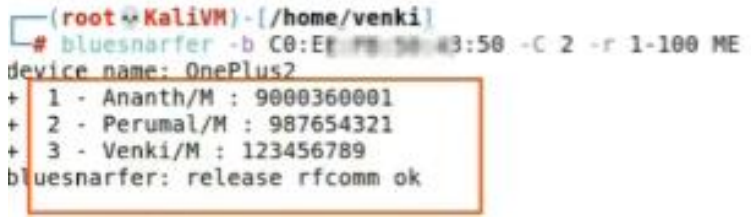
BlueSnarfing

해커가 사용자 몰래 BT 장치와 페어링하여 개인 데이터를 훔치거나 손상시킴
- OBEX Push Profile (OPP) 기능 악용
- OBEX Get Request로 .vcf (주소록) 파일이나 .vcs (달력) 파일과 같이 잘 알려진 파일 확장자를 전송하여 기기 파일에 접근
- 과거에는 명시적으로 페어링되지 않아 가능했지만 현재 PIN 코드 입력 등으로 취약점 보완

* OBEX Push Profile (OPP) : 장치끼리의 데이터 객체 교환에 사용되는 프로토콜
→ 인증 없이 간편하게 정보 전송 가능

Bluesnarfer

> Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant). - https://en.wikipedia.org/wiki/Bluesnarfing



BlueTooth 공격 방식

BlueBugging & BlueJacking

BlueBugging
- 블루투스를 사용하여 피해자의 휴대 전화 또는 PC에 백도어를 설정, 데이터 확인 및 임의의 동작 실행 가능

BlueJacking
= BlueSpamming
– 스팸처럼 익명으로 블루투스 사용자에게 메시지를 전송, 기기 제어가 아닌 단순히 메시지 전송

BlueTooth 취약점

BlueTooth 취약점

BlueBorne (2017)

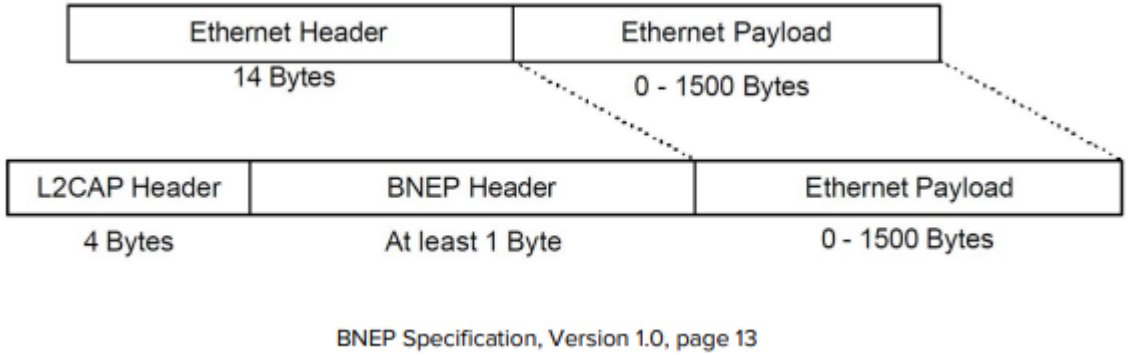
- 8개의 취약점 모음
- 안드로이드, iOS, 윈도우, 리눅스, 사물 인터넷 기기 등 약 53억대 이상의 기기에 영향을 미침
- 블루투스가 활성화되어 있는 장치에 paring하지 않아도 장치 제어 가능
- 아미스(Armis) 연구진이 발견

BlueTooth 취약점

BlueBorne (2017)

안드로이드

(1) CVE-2017-0781 : BNEP (Bluetooth Network Encapsulation Protocol, 테더링)에서 발생하는 원격코드 실행 취약점 (RCE)



BNEP Specification, Version 1.0, page 13

- BNEP (Bluetooth Network Encapsulation Protocol)
  - 블루투스 내에서 IP 기반 네트워크 캡슐화 제공
  - 인터넷 tethering(sharing)을 허가
  - 이더넷 패킷의 다양한 형태를 캡슐화 하여 L2CAP에 연결하는 것이 BNEP 계층의 목적

블루투스 테더링 : 기기와 1대1로 연결하여 데이터를 공유하는 기능
캡슐화 : 상위 계층 데이터를 하위 계층에 보내기 위해 하위 계층 Header로 감싸주는 기술
L2CAP : 중간 계층

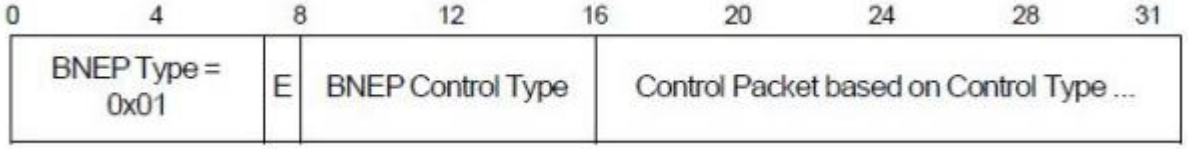
BlueTooth 취약점

BlueBorne (2017)

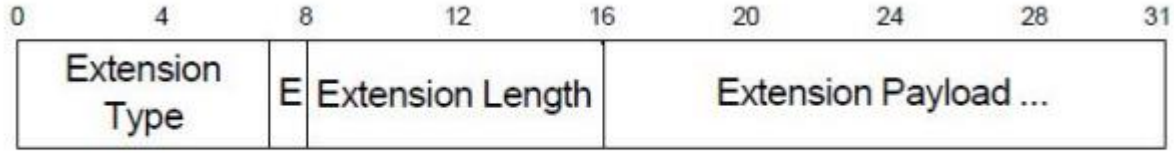
안드로이드

(1) CVE-2017-0781 : BNEP RCE

- BNEP Control message를 사용하면 PAN(Personnal Area Network) 연결 쉽게 가능



- BNEP Extension 가능 : 한 개의 L2CAP 메시지에 여러 개의 BNEP 제어 메시지를 담기 위해 확장 가능



BNEP extension header format, BNEP Specification, Version 1.0, page 39

BlueTooth 취약점

BlueBorne (2017)

안드로이드

(1) CVE-2017-0781 : BNEP RCE

https://www.youtube.com/watch?v=Az-I90RCns8

```
UINT8 *p = (UINT8 *)(p_buf + 1) + p_buf->offset;
...
type = *p++;
extension_present = type >> 7;
type &= 0x7f;
...
switch (type)
{
...
case BNEP_FRAME_CONTROL:
    ctrl_type = *p;
    p = bnep_process_control_packet (p_bcb, p, &rem_len, FALSE);
    if (ctrl_type == BNEP_SETUP_CONNECTION_REQUEST_MSG &&
        p_bcb->con_state != BNEP_STATE_CONNECTED &&
        extension_present && p && rem_len)
    {
        p_bcb->p_pending_data = (BT_HDR *)osi_malloc(rem_len);
        memcpy((UINT8 *)(p_bcb->p_pending_data + 1), p, rem_len);
        ...
    }
...
```

안드로이드의 BNEP 제어 메시지 처리 과정

- BNEP 제어 메시지
- 여러 제어 메시지 처리를 위해 확장 비트를 사용

→ BNEP_SETUP_CONNECTION_REQUEST_MSG 전송

→ 인증 완료 → 연결 완료 → 확장 제어 메시지 분석

- 분석할 제어 메시지
- p_pending_data에 따로 저장
- Memcpy시 p_peding_data +1 진행
- 버퍼 오버플로우 발생

➔ 제어 구문을 악성코드로 전송할 시 오버플로우를 통한 원격 코드 실행 가능

BlueTooth 취약점

BlueBorne (2017)

[안드로이드]

1) CVE-2017-0781 : BNEP (Bluetooth Network Encapsulation Protocol, 테더링)에서 발생하는 원격코드 실행 취약점 RCE
2) CVE-2017-0782 : 안드로이드의 BNEP PAN(Personal Area Networking, IP기반 장치간 네트워크 연결) 프로필에서 발생하는 원격코드 실행 취약점
3) CVE-2017-0783 : 안드로이드의 블루투스 파인애플에서 발생하는 Man-in-the-Middle 공격 취약점 Information leak – 파인애플 (무선 장치 감사 도구)
4) CVE-2017-0785 : 안드로이드 SDP(Service Discovery Protocol, 주변 장치 식별)에서 발생하는 정보 노출 취약점

BlueTooth 취약점

BlueBorne (2017)

[윈도우]

5) CVE-2017-8628 : 윈도우의 블루투스 파인애플에서 발생하는 스푸핑 취약점

[리눅스]

6) CVE-2017-1000251 : 리눅스 블루투스 스택(BlueZ)에서 발생하는 정보노출 취약점
BlueZ : 리눅스 환경에서 Bluetooth 무선 표준 스팩을 구현한 라이브러리

7) CVE-2017-1000250

[애플]

6) CVE-2017-14315 : 애플의 Low Energy 오디오 프로토콜에서 발생하는 원격코드 실행 취약점

➔ 해당 취약점에 영향을 받는 다양한 기업에서 최신 버전으로 취약점 패치 완료

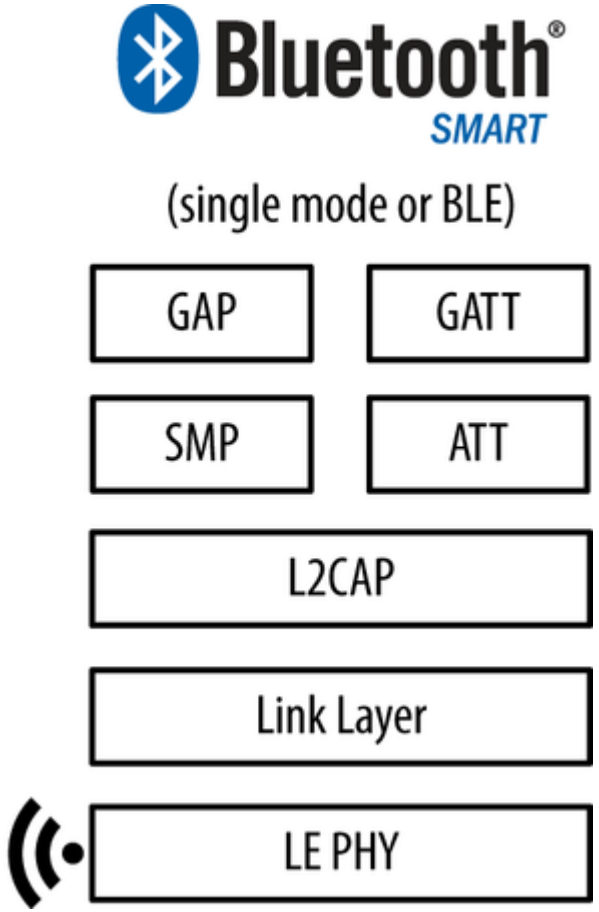
BlueTooth 취약점

BlueTooth 종류

1) 클래식 블루투스 (Classic Bluetooth)
- 1.0부터 2.1로 이어져온 기존 블루투스
- 블루투스 BR/EDR이라고도 부름
- 주로 오디오 관련

2) 고속 블루투스 (Bluetooth HighSpeed)
- 3.0에서 더해진 와이파이를 이용한 고속전송 기술의 연장

3) 저전력 블루투스 (Bluetooth Low Energy)
- 전력 소모를 최소환, 배터리 수명 연장
- 웨어러블 장비 등 널리 사용
- 에너지 효율 높여주고 사용 편리
- Advertising packet을 항상 평문으로 전송



Advertising packet : 기기의 이름, 주소, UUID 등이 들어있음

BlueTooth 취약점

KNOB (2019) – CVE-2019-9506

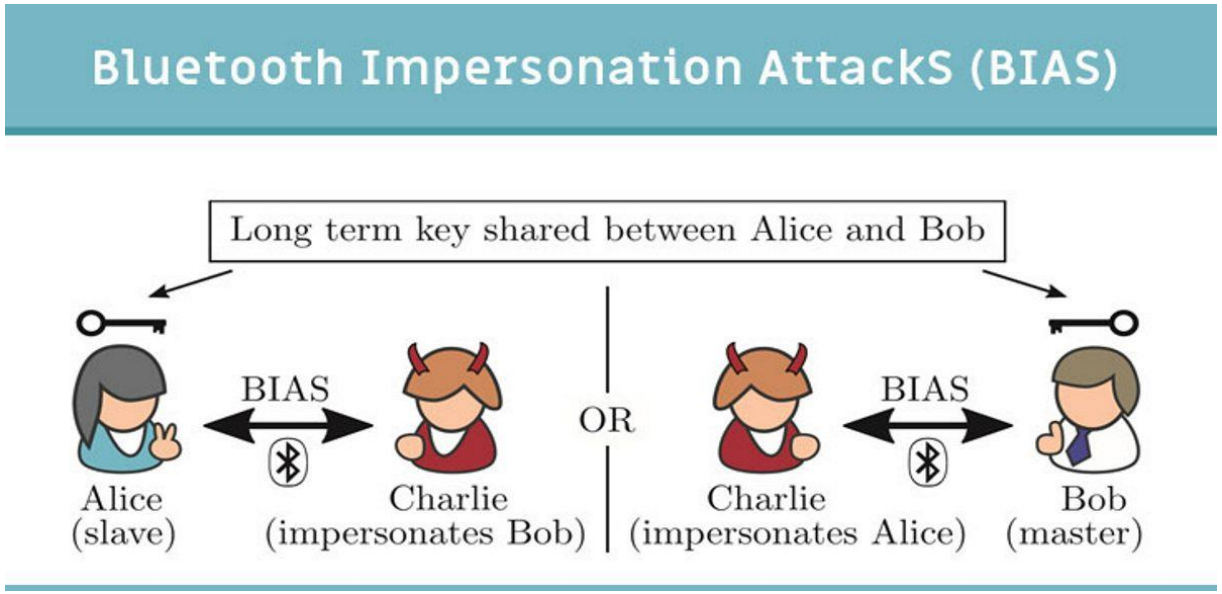
KNOB (Key Negotiation of Bluetooth) 공격
- Bluetooth BR/EDR 대상
- 연결 설정에 사용되는 암호화 키 길이를 single octet으로 감소 가능
- 공격자와 가까운 거리 두 장치 사이 암호화된 블루투스 트래픽 조작 및 가로채기 가능

조건
- 짧은 시간 내에 키 길이 협상 메시지를 가로채고 조작하고 다시 보내는 동시에 두 장치 전송을 모두 차단해야함
- 암호화키 단축, 암호 해독키 강제 해독
- 페이링 할 때마다 공격 반복

대응
- 장치 제조업체, SW 공급 업체가 최소 7 octet 암호화 키 길이 적용 권장

BlueTooth 취약점

BIAS (2020) – CVE-2020-10135



BIAS (Bluetooth Impersonation AttackS)

- 블루투스 사칭 공격
- Bluetooth BR/EDR 대상
- 블루투스 기기가 처음 paring할 때 롱텀(long-term)키 (= 링크키) 생성
- 한번 paring 하면 롱텀키를 세션키처럼 사용하고 다시 paring X
- 해당 롱텀키 생성이 허술함 ➔ 롱텀 키를 몰라도 이전 연결 기기로 속여 연결 가능

→ BIAS와 KNOB를 조합해서 공격하면 안전 인증 모드까지 깰 수 있음

BlueTooth 취약점

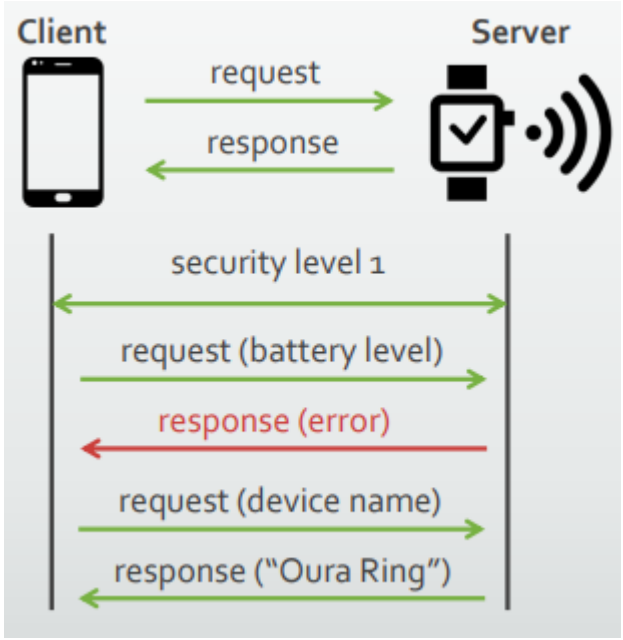
BLESA (2020) – CVE-2020-9770

BLESA (BLE Spoffing Attacks)
- BLE 대상
- 블루투스 재연결 과정에서 발생
- 한번 페어링이 완료되면 추가 인증 없는 것을 악용
- 수십억 대의 IoT에 영향, 안드로이드 장비들은 거의 대부분 이 취약점에 노출된 채 사용

BlueTooth 취약점

BLESA (2020) – CVE-2020-9770

Attribute	Value	Security Requirement
Device Name	"Oura Ring"	Level 1
Battery level	"90%"	Level 2



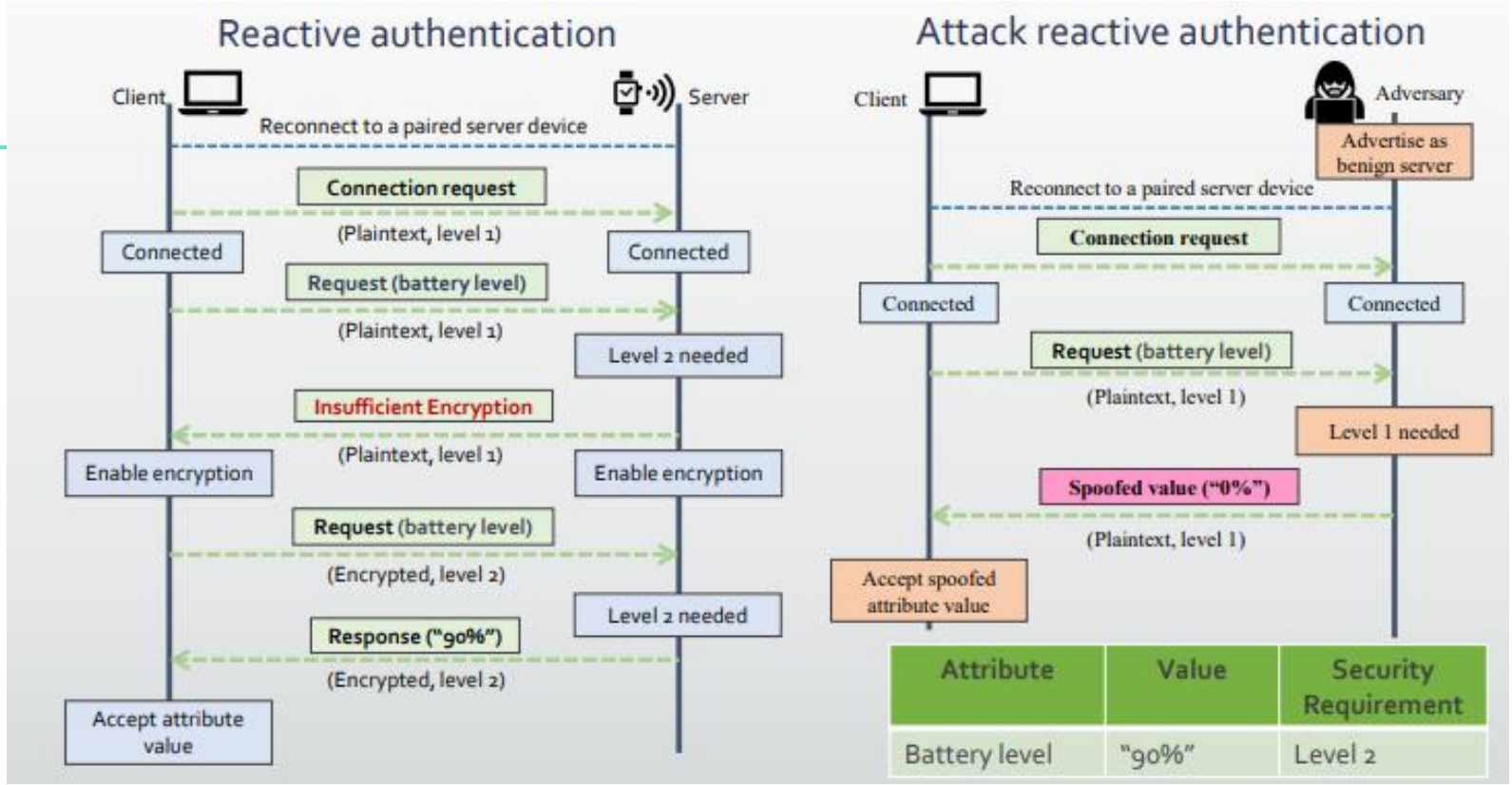
BLE 보안 매커니즘

1) Server-Client Architecture
- BLE는 server, client 구조로 요청과 응답 스키마 사용.
- 서버 장치에 속성 데이터 저장 & 각 속성은 보안 요구사항 존재

2) Server-side Security Enforcement
- 서버는 현재의 보안 레벨이 보안 요구사항과 일치하는지 확인

BlueTooth 취약점

BLESA (2020) – CVE-2020-9770



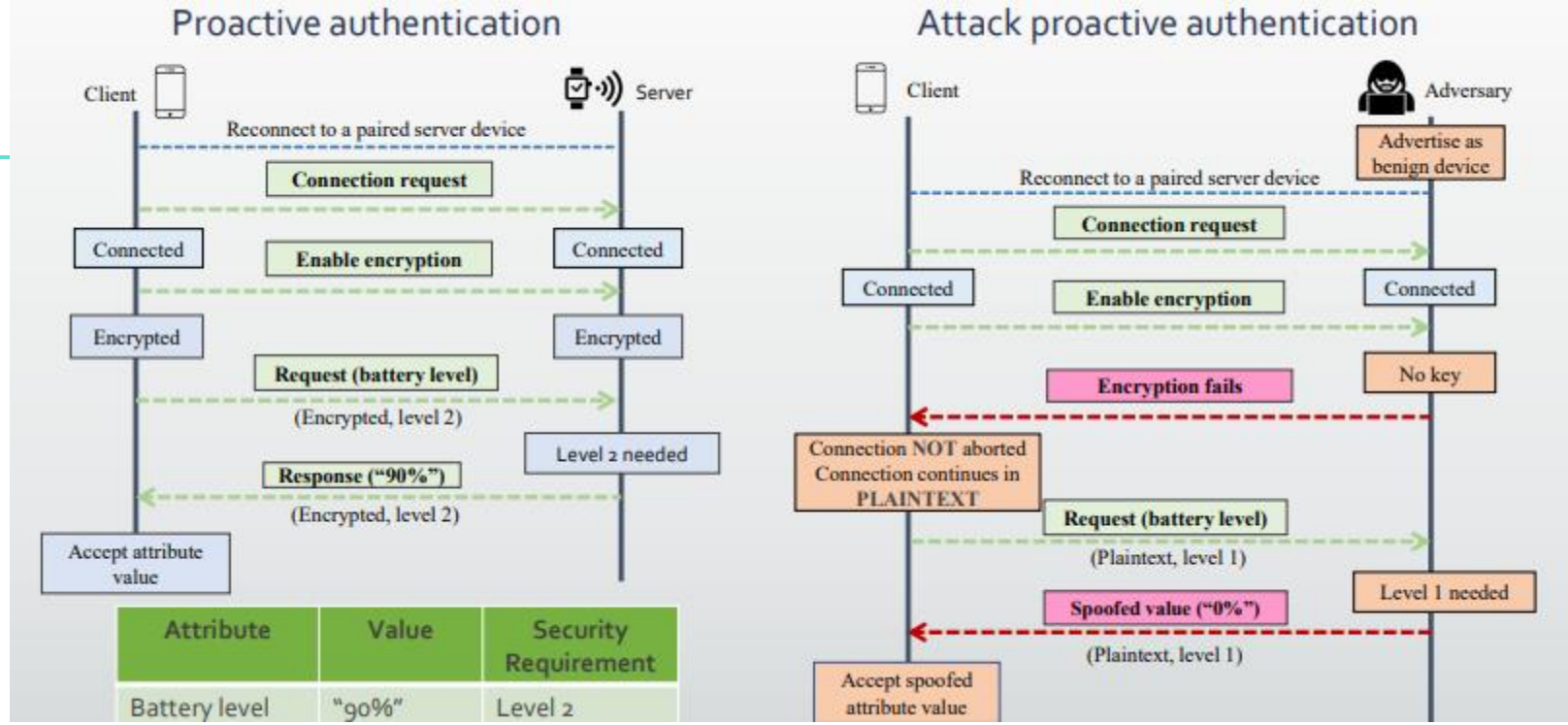
BLE 재 연결시 인증 절차

1) Reactive Authentication
- 재연결을 요청하여 연결된 직후 일반 텍스트 (보안 레벨 1)로 요청을 전송
- 이에 대한 server의 react가 오류 메시지라면 다시 레벨을 올려서 전송하고 응답

공격
- 오류 메시지가 아니기만 하면 Client가 응답을 받아들임
- Client가 서버에게 보낸 요청을 가로채고 스푸핑된 응답을 전송해 Client가 자신과 재 연결하도록 함

BlueTooth 취약점

BLESA (2020) – CVE-2020-9770



BLE 재 연결시 인증 절차

2) Proactive Authentication
- 클라이언트가 서버에 요청을 보내기 전에 암호화/인증을 사전에 활성화함
- 기존에 설정된 사전 공유 비밀키로 암호화 활성화 한 후 인증을 진행
- 서버가 암호화 사용 가능으로 설정하지 않으면 인증 확인에 실패했다고 생각하고 클라이언트는 연결을 중단

공격
- 안드로이드와 ios기반 장치가 절차를 제대로 따르지 않음 ➔ 자원 제약, 서버 장치와 호환성 유지, 사용성 향상
- 암호화 되지 않은 응답에 대해 평문으로 다시 응답하여 속성을 속여
- 전달된 스푸핑 데이터를 client가 연결 해제하지 않고 받아들여 BLESA 취약점이 허용

BlueTooth 취약점

https://www.youtube.com/watch?time_continue=18&v=qPYrLRausSw&feature=emb_title

BleedingTooth (2020) – CVE-2020-12351, 12352, 24490

CVE-2020-12351, 12352 : 인증 과정을 통과하지 않은 사용자가 장비 근처에서 정보에 접근
CVE-2020-24490 : 인증 과정을 통과하지 않은 사용자가 장비 근처에서 디도스 공격

구글과 인텔이 BlueZ에서 취약점 발견
- 리눅스 커널 5.9 이전 버전이 취약점에 노출
- '제로 클릭 공격' 가능 (링크를 클릭하거나 파일을 열지 않아도 됨)
- Type Confusion 취약점
- net/Bluetooth/l2cap_core.c에서 발견
- 코드 실행 or 마비 가능

Type Confusion : 프로그램에서 사용하는 변수나 객체를 선언 혹은 초기화했을 때, 다른 타입으로 사용할 때 발생하는 오류
BlueZ : 리눅스 환경 Bluetooth 무선 표준 스팩 구현 라이브러리

BlueTooth 취약점

BRAKTooth (2021) – 16개의 취약점

BT SoC Vendor	BT SoC	Dev. Kit / Product	Sample Code
Bluetooth 5.2			
Intel	AX200	Laptop Forge15-R	N.A
Qualcomm	WCN3990	Xioami Pocophone F1	N.A
Bluetooth 5.1			
Texas Instruments	CC2564C	CC256XCQFN-EM	SPPDMMultiDemo
Zhuhai Jieli Technology	AC6366C	AC6366C_DEMO_V1.0	app_keyboard
Bluetooth 5.0			
Cypress	CYW20735B1	CYW920735Q60EVB-01	rfcomm_serial_port
Bluetrum Technology	AB5301A	AB32VG1	Default
Zhuhai Jieli Technology	AC6925C	XY-WRBT Module	N.A
Actions Technology	ATS281X	Xiaomi MDZ-36-DB	N.A
Bluetooth 4.2			
Zhuhai Jieli Technology	AC6905X	BT Audio Receiver	N.A
Espressif Systems	ESP32	ESP-WROVER-KIT	bt_spp_acceptor
Bluetooth 4.1			
Harman International	JX25X	JBL TUNE500BT	N.A
Bluetooth 4.0			
Qualcomm	CSR 8811	Laird DVK-BT900-SA	vspspp.server.at
Bluetooth 3.0 + HS			
Silabs	WT32i	DKWT32I-A	ai-6.3.0-1149

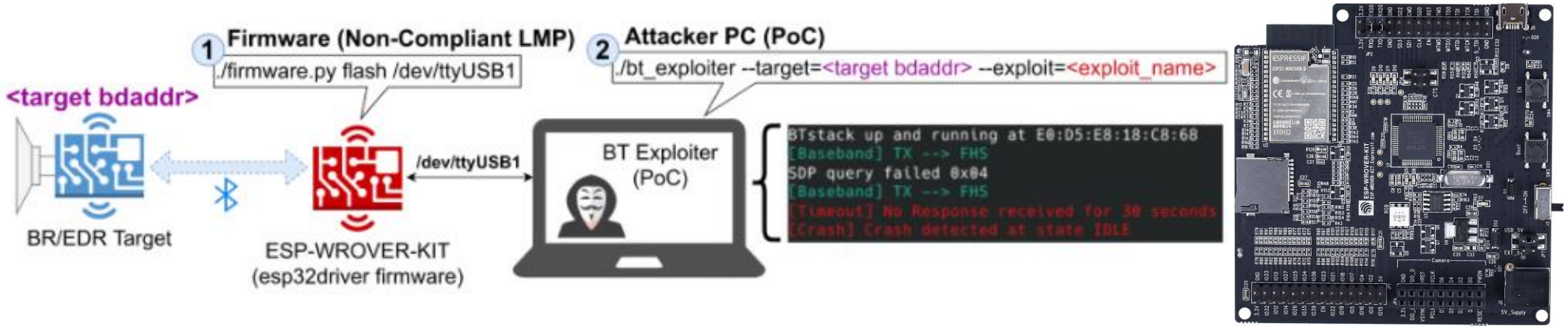
Intel, Qualcomm, Zhuhai Jieli Technology, Texas Instruments와 같은 벤더 11곳의 블루투스 칩셋 13개에 취약점 존재

- 랩탑, 스마트폰, 프로그래머블 로직 컨트롤러, IoT 기기를 포함한 약 1400개 이상의 상용 제품에 사용
- 4개의 취약점은 espressif 시스템과 샤오미로부터 버그 바운티 받음
- BT stack은 여러 제품에서 고유되는 경우 많음 ➔ 다른 많으 제품들이 영향 받을 가능성 높음

BlueTooth 취약점

BRAKTooth (2021) – 16개의 취약점

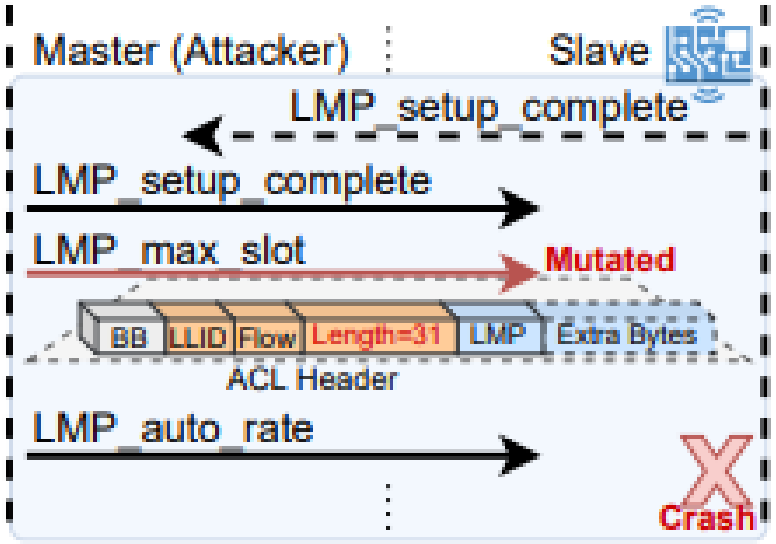
1) CVE-2021-28139
- ESP32 SoC에 존재 : 가전제품에서 산업용 장비까지 많은 기기에 사용
- 라이브러리에 Out-of-Bound 검사 누락으로 발생



Non-Compliant LMP : 사용자 지정 Link Manager Protocol

BlueTooth 취약점

BRAKTooth (2021) – 16개의 취약점



2) CVE-2021-34147

- 인텔 AX200 SoC와 퀄컴 WCN3990 SoC 대상 DoS 공격
- 공격자 페이징 반복, 악성 패킷 전송 등으로 SoC 고갈 가능

→ 고갈된 SoC는 모든 연결 비활성화, 전력 간헐적 차단 등 불안정한 상태로 돌입함.

SoC : System on a chip : 단일 칩에 모든 기능이 집적됨.

BlueTooth 취약점

BRAKTooth (2021) – 16개의 취약점

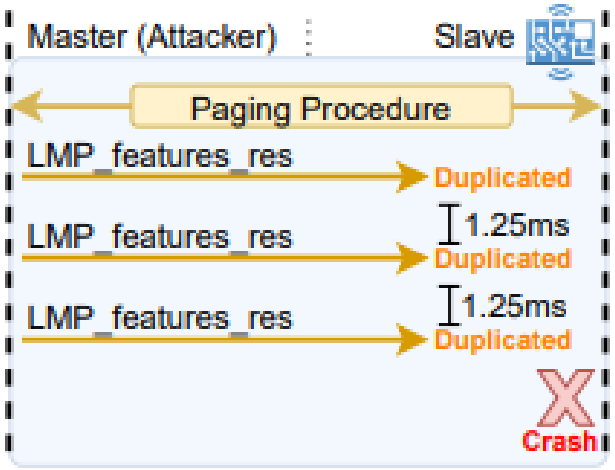


Figure 9: Feature Response Flooding

3) 블루투스 기반 오디오 장비

- 대상 : 샤오미의 포터블 블루투스 스피커인 MDZ-36-DB와 BT 헤드폰, BT 오디오 모듈
- CVE-2021-31609, CVE-2021-31612, CVE-2021-31613, CVE-2021-31611, CVE-2021-28135, CVE-2021-28155, CVE-2021-31717과 같은 취약점들이 발견

오디오 재생이 이뤄지고 있을 때 장비를 멈추게 만들 수 있음

대응 방식

감사합니다