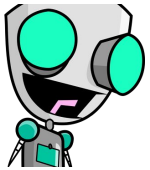
make. hack. void
A Canberra Hackerspace

# Fun with 433MHz

- Other signals in the wild
- Identifying vulnerable (and potentially resistant) systems
- Demonstration of a replay attack
- Getting started


Jamie Reid
@jambulance

Adam Thomas
@dev_dsp

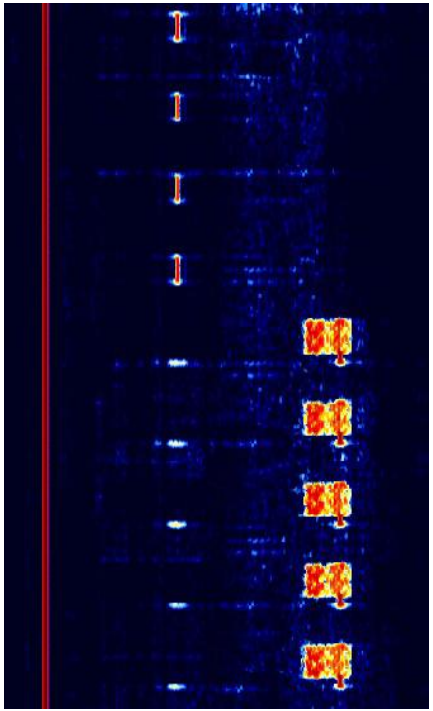


Paul Harvey
@csirac2

# In the wild

- http://www.sigidwiki.com/wiki/Signal_Identification_Guide

  “**CHU** is a time signal radio station operated by the Institute for National Measurement Standards of the National Research Council of Canada”
- https://www.reddit.com/r/signalidentification/
- Foxhunts/DF
- Amateur Radio experiments (weak signal propagation, antenna design, HF/long-distance voice & digital comms, microwave frequency work Eg. 10GHz record=2731km!)
- Bluetooth sniffing
- Debugging/optimizing TV antenna or satellite dish
- As an amateur radio licensee, transmit legally in 27+ bands from 135KHz - 250GHz (2200m - 1.2mm!)

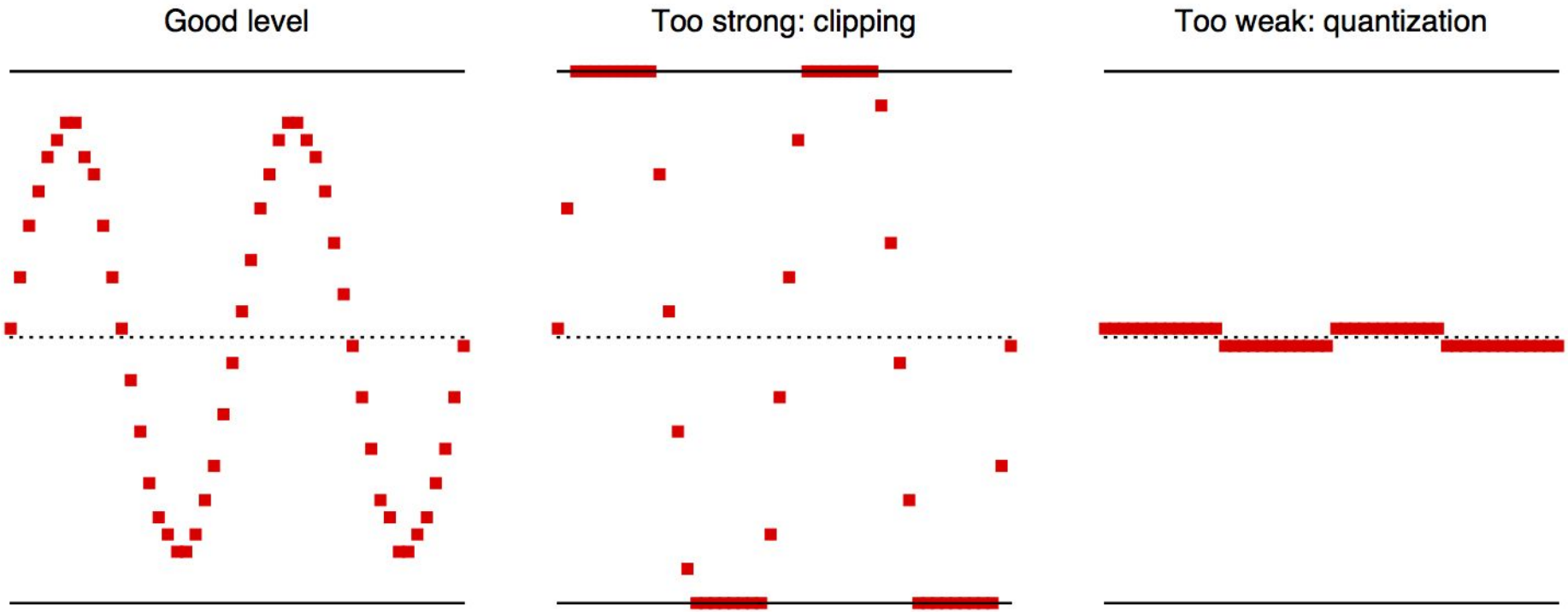


http://www.sigidwiki.com/wiki/CHU

# Boring things (not legal advice)

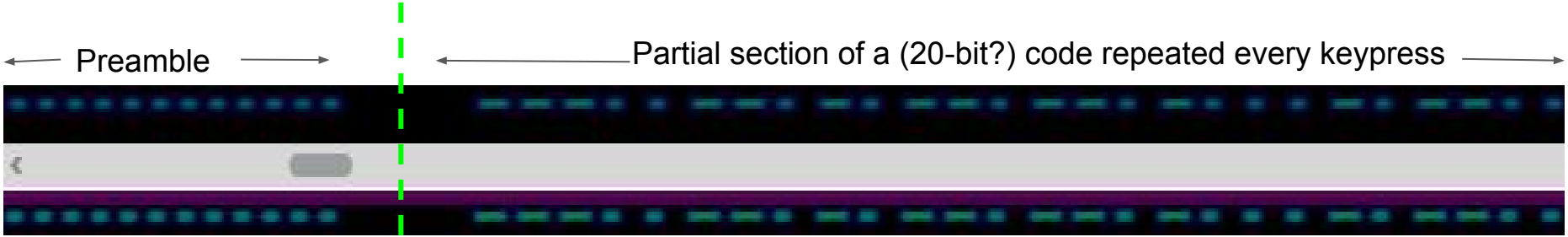
- Nothing gives us the right to make any transmissions over the air, at any power level, other than via provisions of the *Radiocommunications Act 1992*
- All transmissions must be licensed. We don't have "unlicensed" as in the US.
  - Class license - devices are registered, comply to a standard. Burden on device registrant; i.e. sellers/importers who must comply with RCM labelling laws.
    - 27MHz isn't an amateur radio band
    - Some 5GHz WiFi channels licensed exclusively for U-NII outside of ISM & ham bands
    - Supply, possession or operation of non-standard/unlicensed devices = stiff penalties
  - Spectrum license - someone owns a chunk of spectrum -> spectrum owner/operator
  - Apparatus license - individual users
- Frequencies and power levels aren't all that's regulated
  - … just because your amateur license covers a given part of the spectrum doesn't necessarily mean you can use any old modulation, encryption, or occupied bandwidth
  - … makes it hard to reproduce signals like bluetooth, WiFi

# Dynamic range challenges




http://ham.stackexchange.com/questions/2475/why-is-dynamic-range-relevant-for-an-sdr

# Example system vulnerable to trivial replay attack



# Example system not vulnerable to trivial replay attack

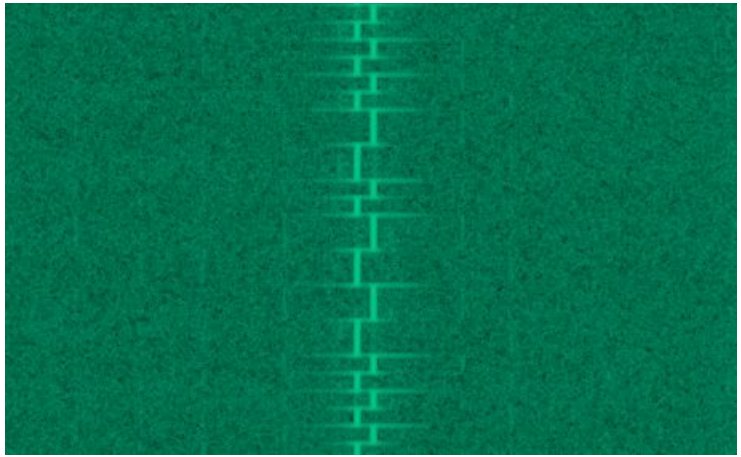
Preamble and ID and/or lock/unlock command (?)

possible rolling code

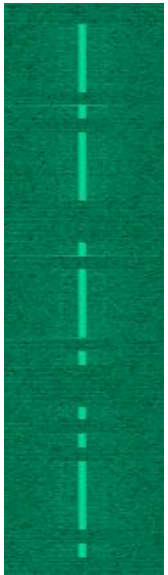
# 433MHz things

- Garage door openers
- Home alarm and automation systems
- Weather stations/wireless thermometers
- Power meters
- Keyfobs

**F**requency[1]
**S**hift
**K**eying



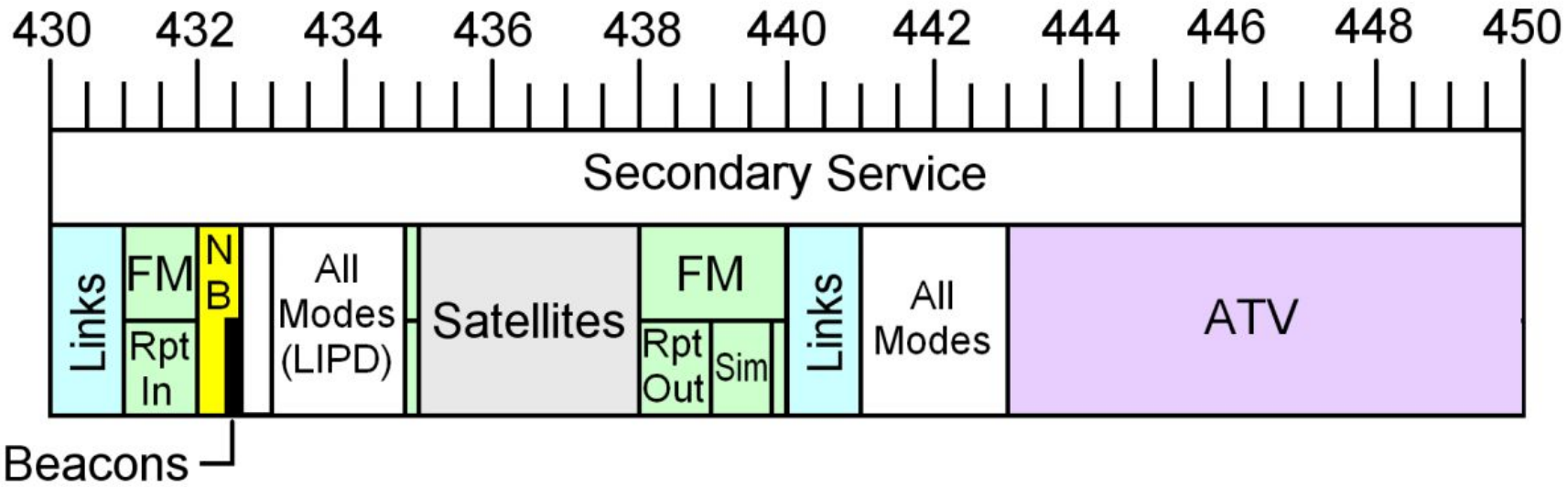
**O**n[1]
**O**ff
**K**eying



1 - http://blog.kismetwireless.net/2013_08_01_archive.html

# 433MHz: can we transmit?

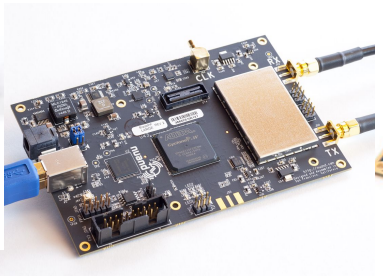
| | | |
|---|---|---|
| 430 - 450 MHz | AMATEUR | Secondary Service |
| 435 - 438 MHz | AMATEUR SATELLITE | Permitted on non-interference basis |



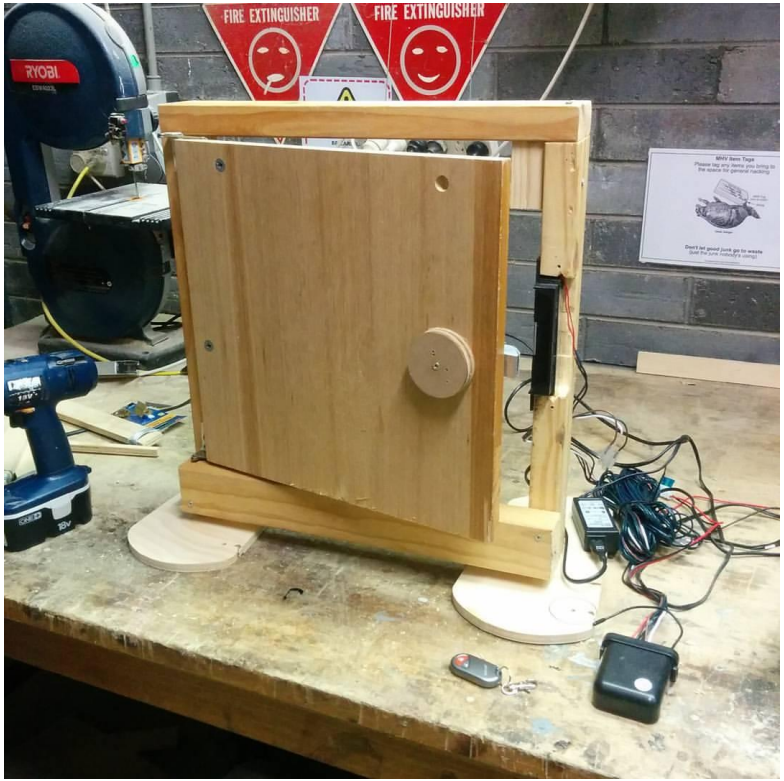

http://www.wia.org.au/members/bandplans/data/documents/Australian%20Band%20Plans%20160211.pdf

# Getting started

- Get an RTL-SDR dongle http://www.rtl-sdr.com/ and play with receiving
- Get a ham radio license!
- Get a transmit-capable SDR
    - Ham-radio specific (friendly, filtered, sensitive, TX power) vs general purpose (BYO DSP & software, BYO filters/amps, noisy/deaf receivers but wide range of operating frequencies)
- Michael Ossman SDR series https://www.youtube.com/watch?v=TZmHgIPBLDo
- http://www.dspguide.com/pdfbook.htm
- http://gnuradio.org/redmine/projects/gnuradio/wiki/SuggestedReading




# Join your local hackerspace & ham radio club




1: https://www.instagram.com/p/BHw9qD2DRcg/

MAKE. HACK. VOID
A Canberra Hackerspace

https://makehackvoid.com/

@makehackvoid

ANU Maker Club

3D printing • shapeable plastic • wood/metal • electronics • coding • sewing • fabrics • CNC • crafts

https://anumaker.club/

CANBERRA REGION AMATEUR RADIO CLUB

http://www.crarc.ampr.org/

Cyberspectrum Melbourne

http://www.meetup.com/Cyberspectrum-melbourne/