What’s on the Wireless?

Automating RF Signal Identification

Dominic Spill
Michael Ossmann

Black Hat USA 2017
Dominic Spill

Senior Security Researcher at Great Scott Gadgets

Open source software developer

HackRF

GreatFET

Ubertooth

@dominicgs
Michael Ossmann

Founder of Great Scott Gadgets

Open source hardware developer

HackRF

GreatFET

Ubertooth

@michaelossmann
Great Scott Gadgets

- HackRF One
- Ubertooth
- YARD Stick One
- GreatFET
For sale on Amazon, hacking gadget that is a car thief’s dream

... and MoS team using it took just two minutes to break into this £100k Range Rover

This problem is only going to get worse

Experts have responded to our investigation by calling for the Home Office to launch a probe into the availability of the HackRF One and similar devices.

Made by Great Scott Gadgets, the HackRF One is marketed for ‘development of modern and next generation radio technologies’. The box displays the disclaimer: ‘You are responsible for using your HackRF One legally.’ However, Andrew Miller, chief technical officer at the motor insurers’ centre ethos Research, said: ‘These gadgets allow for unauthorised keyless entry and are used by criminal gangs to steal vehicles.’

A Land Rover spokesman said: ‘Jaguar Land Rover is concerned about some of the illegal uses of these gadgets by criminal gangs, who are continuously attempting to devise new ways of hacking into vehicles.’
Explanation of terms

Software Defined Radio (SDR) -
   Digital Signal Processing of radio signals

Waterfall - moving spectrogram showing power vs. frequency vs. time

Signal Analysis - Extracting metadata about a given radio signal
   frequency, modulation, bandwidth, duty cycle

Signal Identification - Determining protocol in use by signal analysis

AMC - Automatic Modulation Classification
Waterfall Plots
Waterfall Drawbacks

- Missing transient events
- Limited time displayed
- Limited bandwidth displayed
hackrf_sweep + heatmap.py
Real time visualization demo

QSpectrumAnalyzer

github.com/xmikos/qspectrumanalyzer
Q Spectrum Analyzer
gr-fosphor + hackrf_sweep demo
ShinySDR

Web based tool by Kevin Reid

Waterfall plot, demodulators, band tagging

Can be extended
Automatic Modulation Classification in gr-inspector

8PSK
AM-DSB
AM-SSB
BPSK
CPFSK
GFSK
PAM4
QAM16
QAM64
QPSK
WBFM
Waterfall Drawbacks

Missing transient events

Limited time displayed

Limited bandwidth displayed
Antenna Selection

Sweeping a wide range of frequencies means a wide range of wavelengths

1 MHz / 300 m

6 GHz / 5 cm

Choosing an antenna to cover this range is complicated
Antenna Switching
Direction Finding

Doppler radar

Pseudo-Doppler

Directional antennas

Mike Davis - Cyberspectrum

6:30pm SYN Shop hackerspace
Thanks

Kevin Reid
Mike Walters
Michal Krenek

Great Scott Gadgets Interns:
Jacob Graves
Ellie Puls
Questions?

http://greatscottgadgets.com/spectrummonitoring/

http://greatscottgadgets.com/hackrf/

@dominicgs / @michaelossmann / @GSGlabs