HAM FOR HACKERS

TAKE BACK THE AIRWAVES

JonM – DEFCON 16

JonM

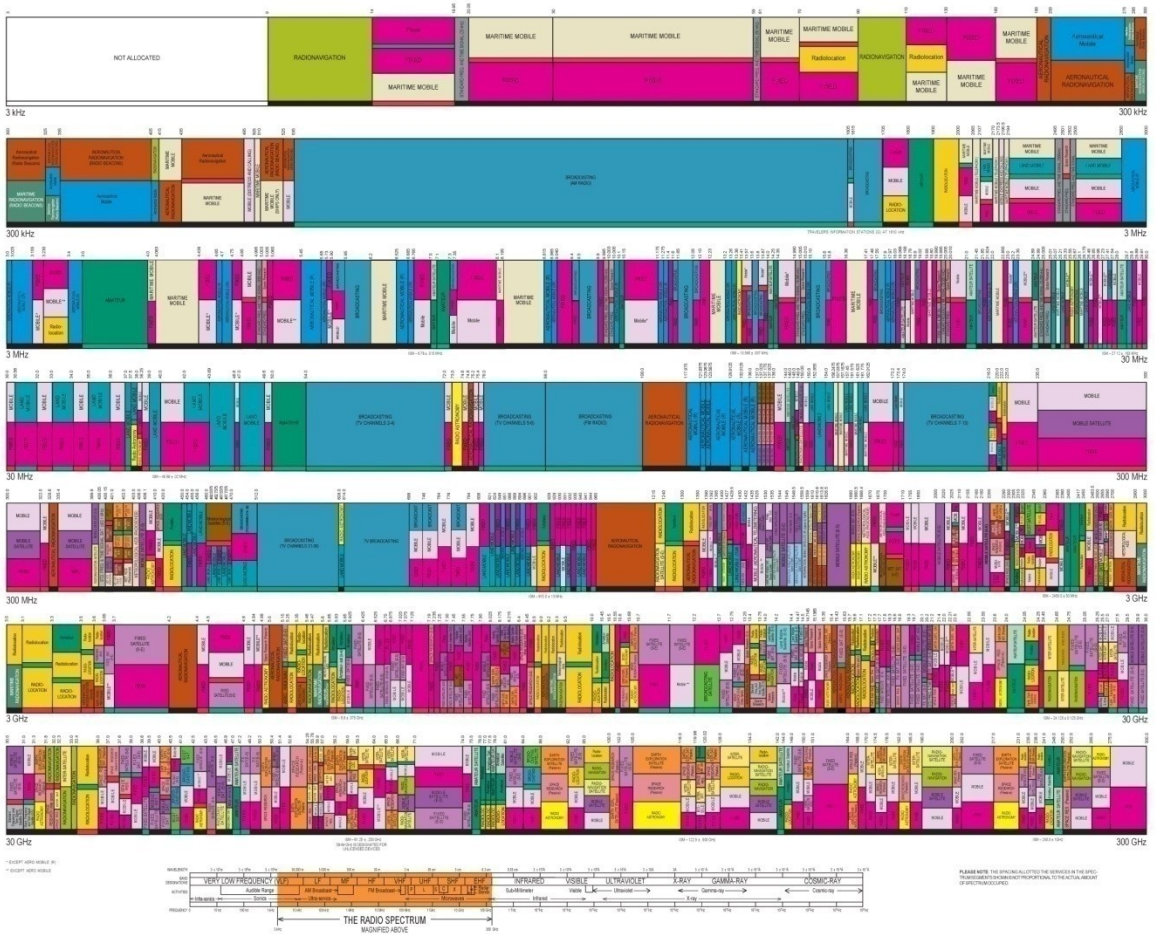
- Licensed Amateur Extra—the highest class of license in the US
- Operating since 2000
- Radio is just one of my hobbies…software security consulting is the most lucrative

You want to play with wireless…

- Remote control
- Data links
- Personal communication
- Telemetry

So what are your options?

US Frequency Allocation



None if it is free for general use



Listening is unrestricted

Aside from some asinine restrictions on analog cell phone frequencies, you can listen to whatever you like all day long.

So what can you use?

- FCC Part 95: Personal Radio Services
  - CB and FRS
  - Low power, short range (couple of miles), voice only
  - Small number of channels
- FCC Part 15: Unlicensed RF Devices
  - WiFi, garage door openers, cordless phones, etc
  - Limited power
  - Antenna restrictions
  - A number of frequencies available, but lots of users

Long story short

- Unlicensed operations are restricted
- You're not going to get much range
- You're going to have a lot of competition
- If there's interference, you have to take it
- If you're interfering with someone else, you have to shut down your transmitter

Enter amateur radio

- FCC Part 97: Amateur Radio Service
- Upsides:
  - You get to use a lot more power
  - You have primary use on a number of bands
- Downsides:
  - You have to be licensed
  - You have to follow operating procedures

Created for Hackers

The FCC's stated principles for amateur radio include:

"Continuation and extension of the amateur's proven ability to contribute to the advancement of the radio art."

Amateur radio was created to provide skilled individuals with a forum for experimentation and technical advancement.

Amateur Radio Limitations

- With great power comes great responsibility:
  - You have to identify yourself
  - No secrecy, no encryption
  - You can't broadcast, especially not music
  - "Non-pecuniary"—non-commercial use only

Oh, one more thing…

You can't swear.

Seriously.

Licensing

- Three levels of license: Technician, General, Extra
- If you just want to experiment, the Technician (lowest) license will get you plenty:
  - Full privileges on the bands above 50 MHz
  - 1500 watts of power!
  - Unlimited bandwidth above 902 MHz
- The higher classes give you access to the HF bands
  - 30 MHz and below
  - Long range, even with low power

Testing

- Tests are multiple choice
  - The entire question pool is published
  - 75% is a passing grade
  - Technician exam is only 35 questions
- You don't have to know Morse code

But isn't ham for losers?

I know what you're thinking:

Ham radio is full of old men who wear suspenders and sit around talking about what they're going to buy when they go into the city.

Well…yes.

These



Folks



Exist



You don’t have to wear suspenders

As long as you’re following the rules and keep to yourself, they’ll leave you alone.

And besides, some of them are actually pretty damn smart.

And isn't the technology outdated?

- Well, yes:

Handheld radio	Cell phone
	
FM modulation	High quality, efficient, codecs
Analog signaling	Digital signaling
Single frequency at a time	Frequency hopping, spread spectrum
Spectrum inefficient–One transmitter at a time	Multiplexing allows multiple transmitters access at once

But there's lots of cool stuff

- Things I've done:
  - Cross country contacts using amateur satellites
  - Tracked a high altitude balloon on the edge of space
  - Picked up signals from the east coast with $20 of hardware
  - Added emergency location beaconing to my motorcycle

New Technologies

- Spread Spectrum
- Digital modes
- Software Defined Radio (SDR)

Spread Spectrum

- Instead of one fat signal, transmit using several smaller signals
- Less interference, more bandwidth, more reliable
- There was a peak of interest in the amateur radio community in the late ‘90s
- Since then, interest has waned
- All of the kits for SS are out of production

Digital modes

D-STAR is a new standard for digital communication

- Basically an ATM implementation
- Up to 128 kbps data rate, over long distances
- 4800 bps digital voice
  - Uses the proprietary AMBE codec (boo)
- A plethora of add-on data services
  - Position reporting
  - Image transfer
  - Text messaging
- Only ICOM is making D-STAR radios right now

Software Defined Radio

- Instead of doing signal processing in hardware, do it in software
- Makes for a much more versatile radio
- New modulation schemes are just software patches
- You can implement powerful filtering and decoding algorithms, too
- Because software does the heavy lifting, hardware becomes much cheaper

GNU Radio

- Open source SDR project
- Uses the Universal Software Radio Peripheral
  - Basically an FPGA, some high quality DACs and ADCs, and a daughterboard interface
  - The daughterboards handle the RF detection and generation
  - Daughterboards give coverage from 0-2.4 GHz
- Support for many different modulations, encodings, etc.
- At $700 for the base USRP, not inexpensive

USRP, expensive?

- $700, plus an extra $150 for RF modules, just for a radio?
- Yeah, but it gives you most of the functionality of this here $13,000 radio:



HP SDR

- Like the USRP, a modular SDR platform
- Stronger amateur radio focus than USRP, but hardware is designed to be modular and versatile
- Still in development, backplane and several boards available now
- Price for a full 0-55 MHz SDR transceiver should be in the $800 range

I/Q demodulation

- Ditch the FPGA, and use the analog hardware you've already got
- Use a cheap board to grab a chunk of spectrum, and feed it into your soundcard
- Software then performs demodulation and decoding
- Bandwidth is limited by your soundcard
- Frequency is limited by what you can generate cleanly
  - 50 MHz is the practical limit for low-cost hardware

SoftRock radios

- Low cost kits:
  - $10 single band receiver
  - $30 single band transceiver
  - $42 frequency agile receiver
- A variety of software packages to process the signals

Go from this:

Tune across the band.

Find a signal.

Copy the morse code down to paper.

You do know morse, right?

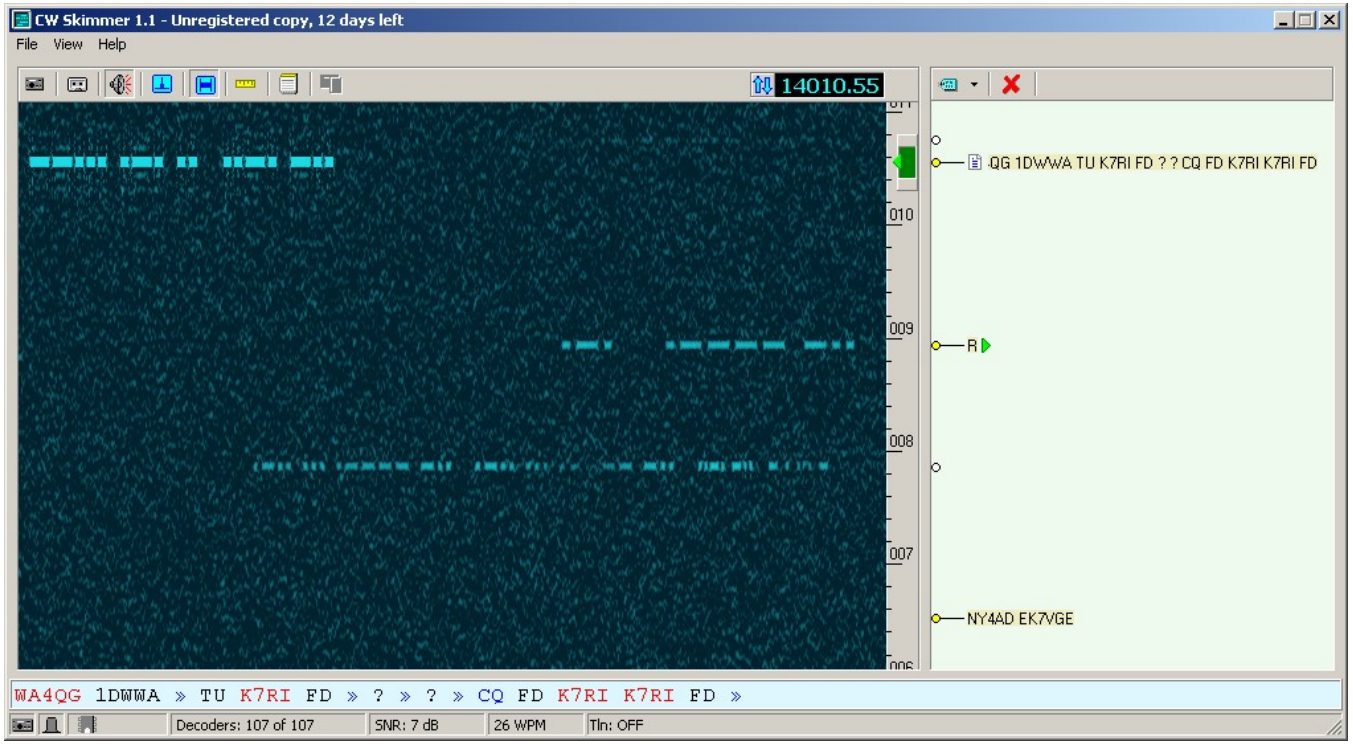


To this:

Start the software.

See the morse scroll across the screen.

Scroll through the spectrum, and read the text.



Call to arms

- Hams are stuck using ancient technology
- But they're all dying off (literally)
- When they go away, so will their spectrum
- They’re not making good use of it anyways
- Let's keep that spectrum open for experimentation, and do cool things with it

We can make it better…

…just by using existing technologies we all know and love.

- More efficient spectrum use
- Higher data rates
- D-STAR is just TCP/IP reinvented, and is built around a restricted technology
- SDR opens a wealth of possibilities

What next?

- Get your license!
- Start experimenting
  - Build some kits
  - Play with software
  - Repurpose existing hardware
- Bring amateur radio back into the realm of hackers and experimenters

Questions?

JonM <jammer@weak.org>