Theory and Practice of Intercepting Radio Voice Transmissions

By Dan Tennery-Spalding, K6XCX
dan@danrad.io

Goal

To be able to intercept and understand radio voice comms.

- Scoped to radio-to-radio (simplex) unencrypted comms.
- We will get you started on your journey!

Hypothetical Scenario

You are the blue team.

The red team is role playing an armed gang that is invading your community.

Blue team goal is to intercept their comms to gather intelligence.

Premise 1 of 3

Radio comms is different from all others. The speaker doesn’t know if who they’re talking to:

- is listening,
- in range,
- able to understand,
- able to respond…
- Or who else is listening!

Premise 2 of 3

To cope with these limitations, radio operators have developed their own lingo and protocols

If you don’t understand them, you won’t understand what you hear, even if you intercept 100% of it

The best way to understand radio lingo and protocols is to use them yourself

Premise 3 of 3

The basics of signal interception are not hard. The hard parts are:

- Developing an intuition around how radio waves propagate
- Understanding what’s being said in real time

We Won’t Cover

Encryption

Digital radio

Trunking systems

Mesh networks

Signal spoofing

Deliberate interference

An Incomplete List of Radio Rules (US Edition)

Can’t transmit GMRS or Ham without a license

Can’t deliberately interfere with someone else’s transmissions

Can’t use encryption (LoRa, i.e. Meshtastic, excepted)

Can’t decrypt protected transmissions

Can’t necessarily record or divulge intercepted transmissions

Note: There are many more rules, and many exceptions, too

Intro to SDRs (Software Defined Radio)

SDR is often done with a dongle and antenna (~$50) and open-source software

The SDR dongle changes radio signals to 1s and 0s

Once you know what band someone is on, it can be easy to find their frequency

When you look at someone's radio you can make an educated guess

- A cop radio is going to work on frequencies allocated to public safety
- Note: Some radios can do both GMRS and Ham
- You can use process of elimination if your first guess isn't right

SDRs and their Software

The software on your computer (Windows or Linux, including Pi's) decodes the 1s and 0s from the SDR dongle into human-intelligible information

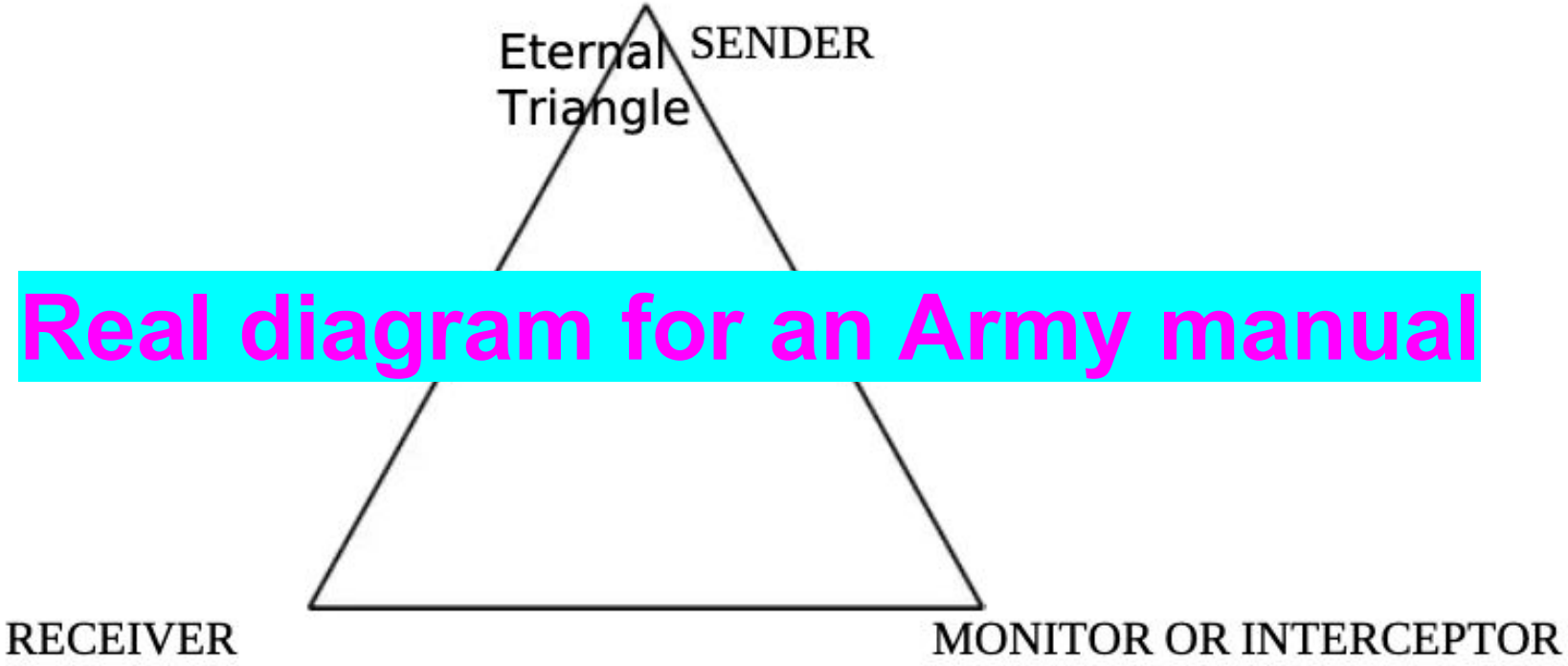
The software can provide a waterfall or other displays

It can also decode different kinds of transmissions: AM, FM, trunked, etc.

It's not hard, but it is complicated

Send screenshots to Claude if it's not working for you

- Or, if you hate AI, don't, and ask a radio nerd community member instead!



Real diagram for an Army manual

Signal Interception 101

The 101: Detect a signal, tune to it, listen, and locate its source if necessary

How can you identify where, on the radio spectrum, to look for the signal?

- You can make an educated guess about what “band” they’re on

You can use a directional antenna

- Concentrates range: Longer range in a narrower area
- Gives you the *direction* of the transmission, not the *location*
- Most common directional antenna is called a Yagi or Yagi-Uda

The Problem “Radio Etiquette” Solves

Every frequency is shared with every other user in range

You cannot transmit only to the person you want to talk to

You don't know if they’re listening, or who else is listening, or if you can reach them, or if it’s intelligible once it does, or whether they can reach you!

Radio users developed "radio etiquette" to communicate effectively

Radio Etiquette Basic Overview

1. Listen before speaking (transmitting)
2. Say the name or callsign of the party you're talking to 3x, then your own
    a. This is so they know to listen, and everyone else knows they don't have to
3. Say *one idea* per transmission
4. End with "Over" if you expect a response, "Out" if not

Real-World Applications

The same skills can be used to capture unencrypted, simplex voice radio comms can be used for encrypted transmissions, digital transmissions, trunking systems and more.

The fundamentals – scan a band, ID a signal, capture and locate it – are the same for any type of transmission.

(Legal) Security-by-Obscurity Options

Low-power transmission

Narrowband transmission

Short and / or infrequent transmissions

Directional antennas

Using unpopular bands

Using terrain and buildings to limit – or redirect – propagation

Bouncing between frequencies and/or bands

Speaking with minimal context

Conclusion

1. Radio operators use lingo and protocols due to radio's unique communication constraints
2. Understanding the lingo and protocols is key to effectively using intercepted transmissions in real time
3. The steps to interception are: ID band used, detect signals in that band, listen and locate (if necessary)
4. Interception tools include SDRs and directional antennas
5. There are numerous legal security by obscurity options

Thank You!

Thank you, BSidesPDX organizers!

You can find my professional site at https://danrad.io

- Email dan@danrad.io
- Contact me if you're interested in a workshop or training