Going Meta

Pulling Info from Encrypted Radios

Luke Berndt – Jan 13, 2024

I am not qualified…

NOT an RF Ninja 🥷

NOT a Security Pro 👩‍💻

NOT a Data Scientist 👩‍🔬

… but I got this to work

AND YOU CAN TOO! 🫵

I hope to provide…

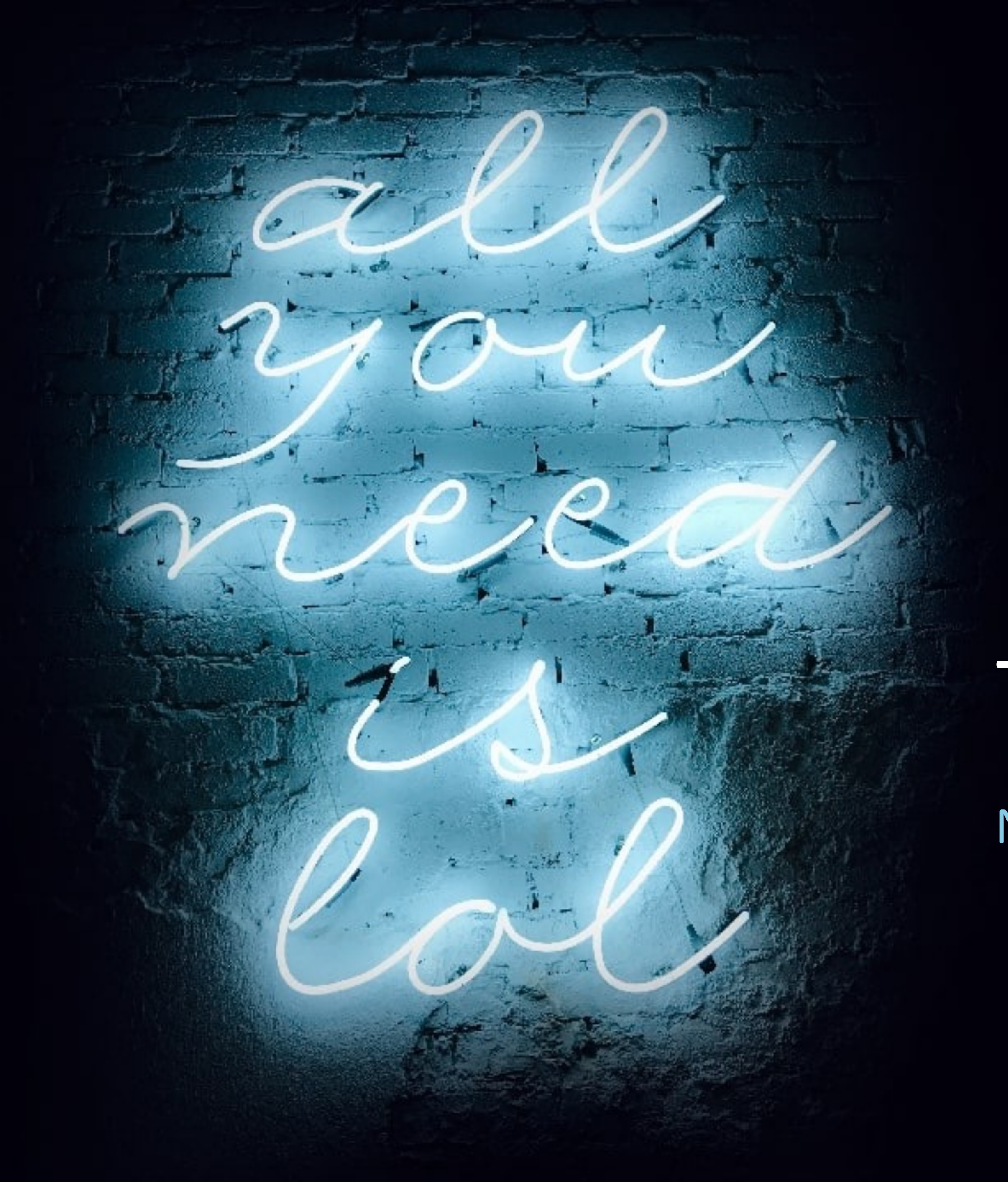
- Understanding of Trunked Radio systems
- Different tools and resources you can use… including Trunk Recorder!
- The type of data you can extract and ways it can be used
- The courage to give it a try

Giants all the way Down…

All of my work is only possible because of other peoples great

I tried to call out what I have built on

(Standing on the Shoulder of Giants + Turtles All the Way Down)

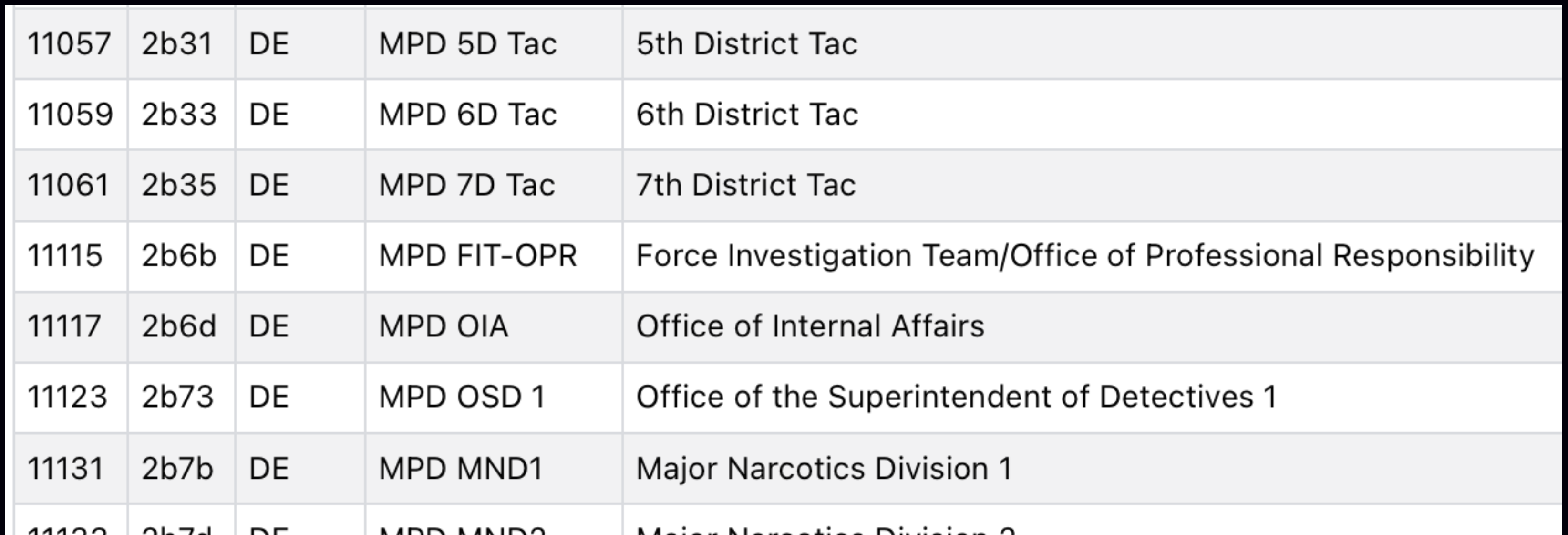


Trunking 101

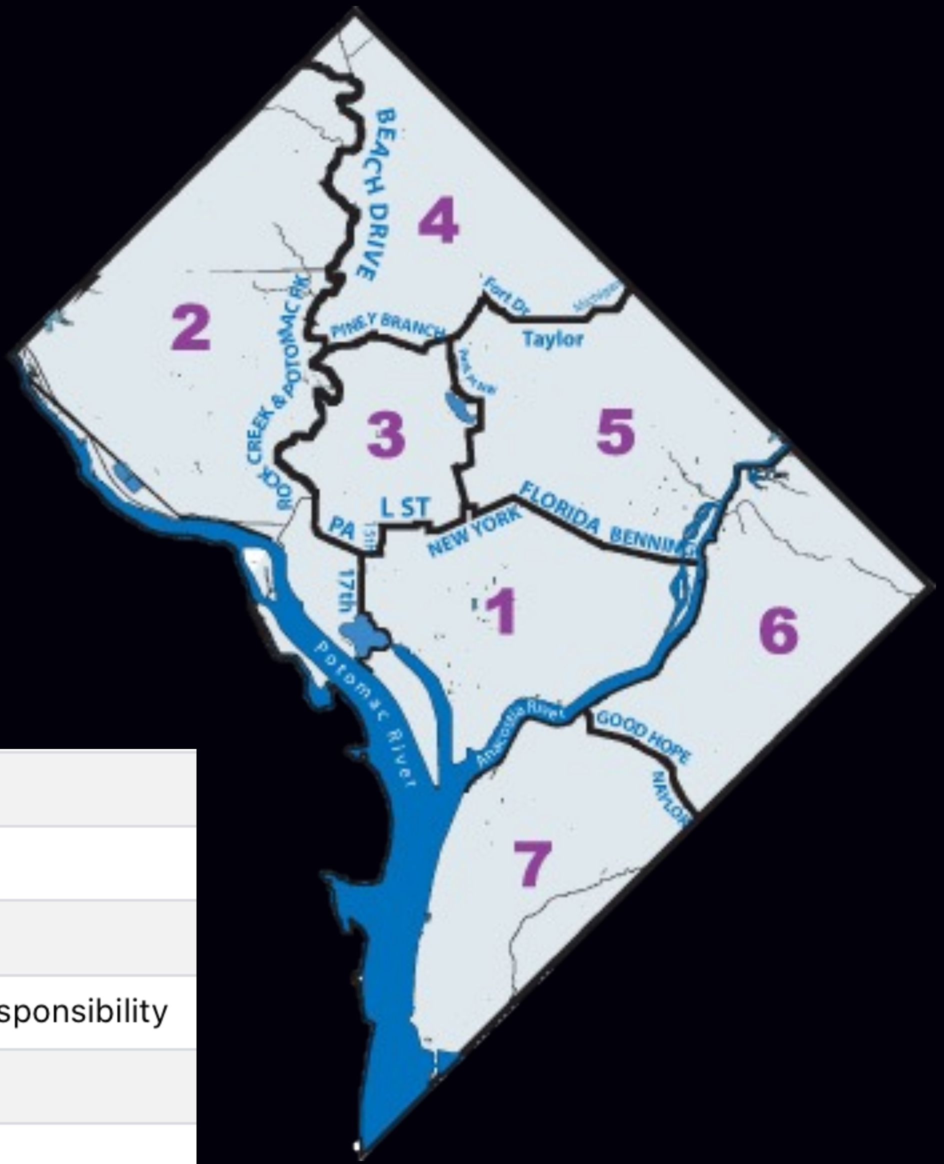
Not only for Elephants

Talkgroups

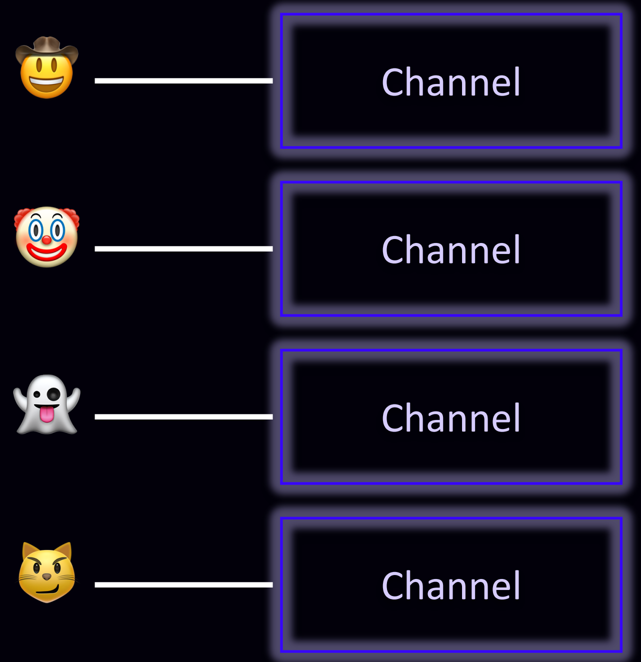
- Organize conversations
- Topical & Geographic
- Gives you clues about who is talking/listening



11057	2b31	DE	MPD 5D Tac	5th District Tac
11059	2b33	DE	MPD 6D Tac	6th District Tac
11061	2b35	DE	MPD 7D Tac	7th District Tac
11115	2b6b	DE	MPD FIT-OPR	Force Investigation Team/Office of Professional Responsibility
11117	2b6d	DE	MPD OIA	Office of Internal Affairs
11123	2b73	DE	MPD OSD 1	Office of the Superintendent of Detectives 1
11131	2b7b	DE	MPD MND1	Major Narcotics Division 1
11133	2b7d	DE	MPD MND2	Major Narcotics Division 2

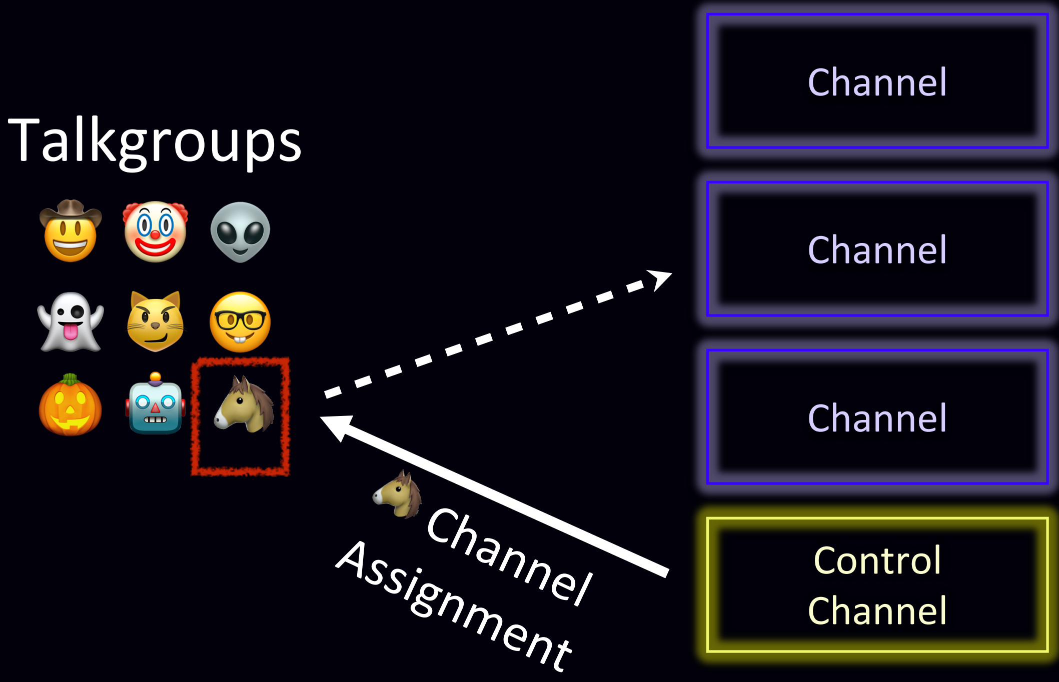


Conventional



Static, fixed channel allocations

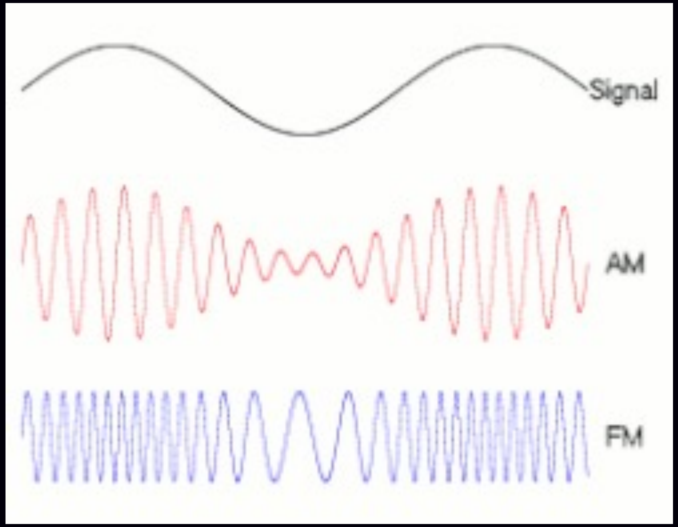
Trunking



- Dynamic channel allocation
- Assigned for each transmission

More talkgroups than channels!

Modulation

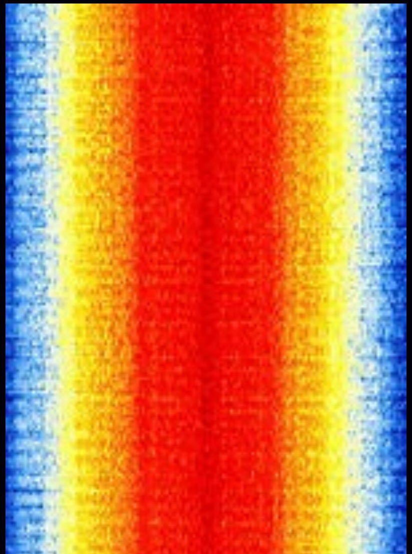


Analog

Speech is directly encoded into the RF signal

Digital

Speech is digitized, and this data is encoded into the RF signal



P25 Transmission
C4FM Modulation
SigIDWiki

Project 25

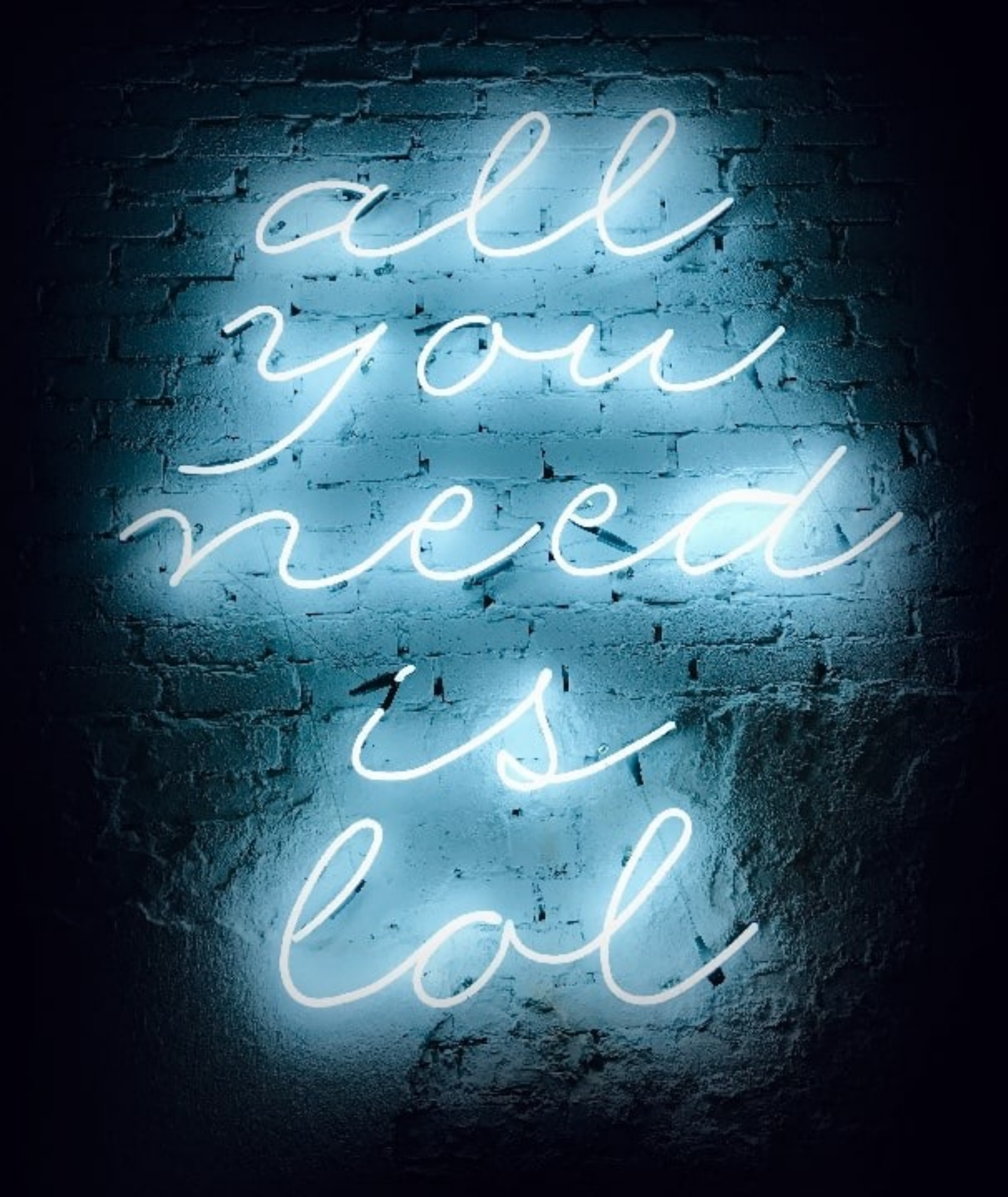
- Standard for digital radios
  - Interoperability & Efficient Market
- Mostly US, mostly government – local, state, Federal, DoD
- Standards effort was kicked off in 1989
- Users drove requirements, radio companies collaboratively designed
  - *(Checkov security gun)*
- P25 US market has a projected revenue of $289.45 Million in 2025

UNITED STATES APCO-25/P25 PUBLIC SAFETY LAND MOBILE RADIO SYSTEMS MARKET 2022
REPORT OCEAN

Project 25

	Analog	Digital
Conventional		👍
Trunked		👍

What we are going to talk about



How I Got Started

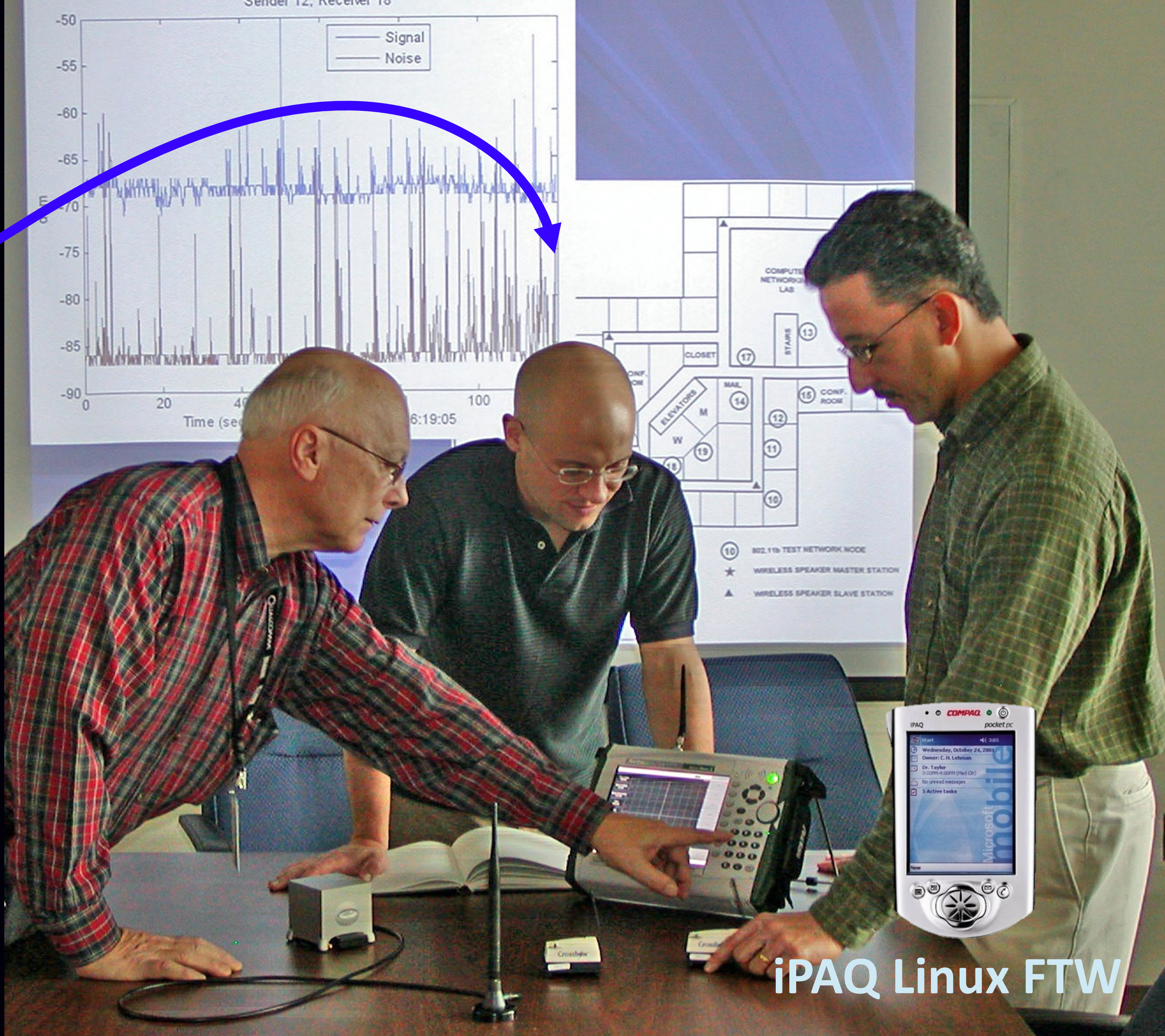
IQ & You

Origin Story!

Luke at his first job, at NIST circa 2002

Public Safety Interoperability

Technically, his first job was a paper route, but it doesn't fit the story as well. Also, there was a brief stint at Radio Shack.



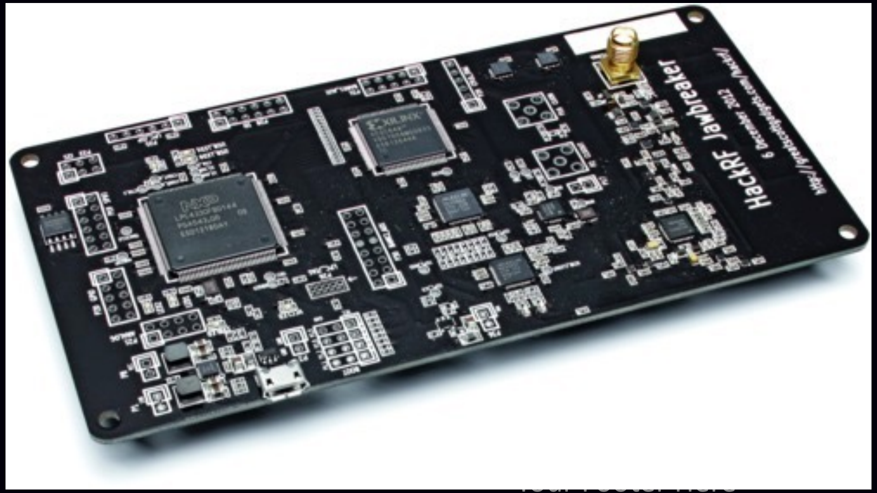
iPAQ Linux FTW

Got to work with Mike Ossmann

Got a free Software Defined Radio…

→

+ DARPA =



HackRF Jawbreaker

150 were given away

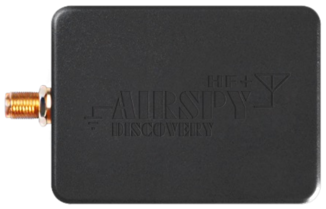
Sweet, gotta free SDR, now what?

Scanners tune in a single frequency and only let you listen to one talkgroup/channel at a time.

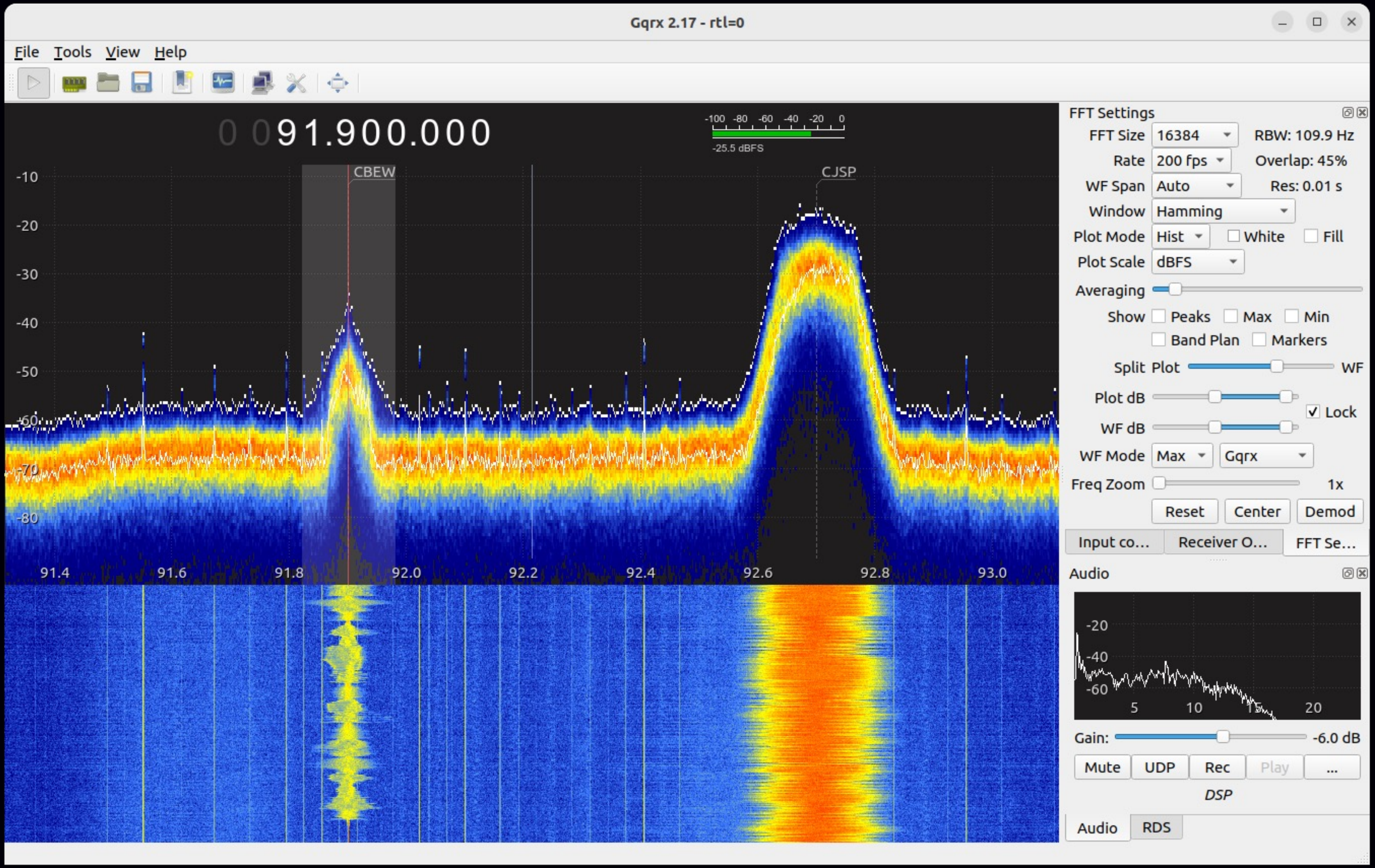
SDRs can capture entire swaths of spectrum, why not record an entire radio system?

Inspired by a post in 2011 by Rachel Kroll
RachelByTheBay.com

Software Defined Radios

Entry	**Wider Bandwidth**	**TX/RX**	**Pro**	**Nation State**
				
RTL-SDR dongles	Airspy, SDRPlay	HackRF, BladeRF, PlutoSDR, LimeSDR	Ettus Networked Series	Per Vices
• **$35** • **2.4MHz** • **RX only** • **8-bit**	• $150 • 10MHz • RX only • 12-bit	• $350 - $700 • 20 - 40MHz • TX & RX • Multi-channel • FPGA	• $10K+ • 100MHz+ • TX & RX • Multi-Channel • FPGAs++	• $100K+ • 1GHz – 3GHz • TX & RX

RF Exploration- GQRX



FFT Settings

FFT Size 16384 RBW: 109.9 Hz

Rate 200 fps Overlap: 45%

WF Span Auto Res: 0.01 s

Window Hamming

Plot Mode Hist □ White □ Fill

Plot Scale dBFS

Averaging

Show □ Peaks □ Max □ Min

□ Band Plan □ Markers

Split Plot WF

Plot dB ☑ Lock

WF dB

WF Mode Max Gqrx

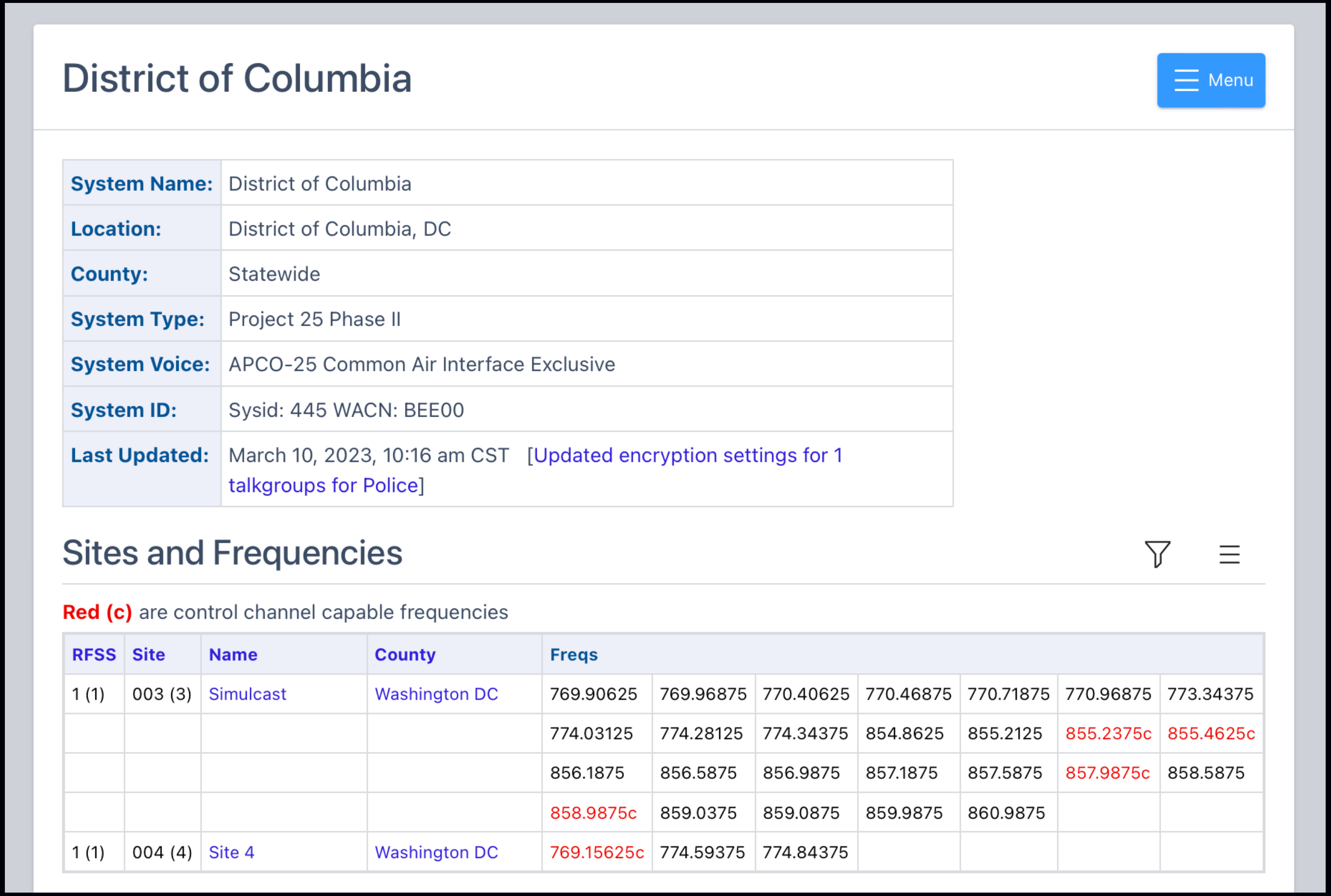
Freq Zoom 1x

Gain: -6.0 dB

- Scroll through the RF Spectrum
- Visual spot and identify signals
- Analog Demod – Listen and also identify
- Capture and Stream signals

https://www.gqrx.dk

Radio Reference



District of Columbia

System Name:	District of Columbia
Location:	District of Columbia, DC
County:	Statewide
System Type:	Project 25 Phase II
System Voice:	APCO-25 Common Air Interface Exclusive
System ID:	Sysid: 445 WACN: BEE00
Last Updated:	March 10, 2023, 10:16 am CST [Updated encryption settings for 1 talkgroups for Police]

Sites and Frequencies

Red (c) are control channel capable frequencies

RFSS	Site	Name	County	Freqs						
1 (1)	003 (3)	Simulcast	Washington DC	769.90625	769.96875	770.40625	770.46875	770.71875	770.96875	773.34375
				774.03125	774.28125	774.34375	854.8625	855.2125	855.2375c	855.4625c
				856.1875	856.5875	856.9875	857.1875	857.5875	857.9875c	858.5875
				858.9875c	859.0375	859.0875	859.9875	860.9875		
1 (1)	004 (4)	Site 4	Washington DC	769.15625c	774.59375	774.84375				

- Crowd sourced radio system information
- System type & frequencies
- Talkgroup numbers and descriptions

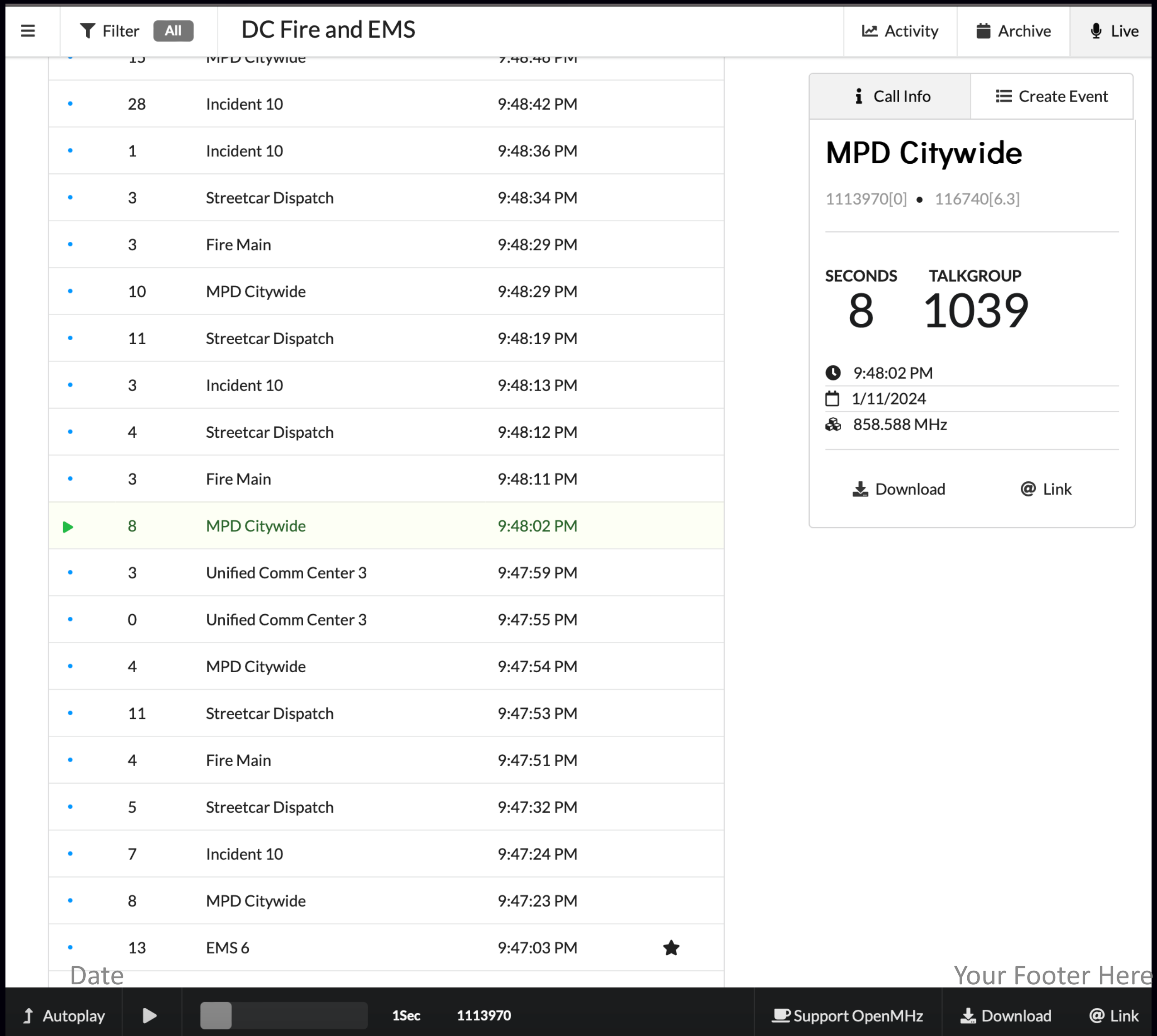
https://www.radioreference.com/db/

Trunk Recorder

https://github.com/robotastic/trunk-recorder

- **My labor of Love**
- Captures all of the transmissions on a Trunked Radio system.
- Started in 2013… so 10+ years of life
- Captures:
  - conventional analog, P25 & DMR
  - trunked SmartNet & P25 Phase 1 & 2
- Built on top of GNU Radio, gr-smartnet & OP25
- Runs on Linux & Macs

OpenMHz.com



DC Fire and EMS

•	15	MPD Citywide	9:48:46 PM	
•	28	Incident 10	9:48:42 PM	
•	1	Incident 10	9:48:36 PM	
•	3	Streetcar Dispatch	9:48:34 PM	
•	3	Fire Main	9:48:29 PM	
•	10	MPD Citywide	9:48:29 PM	
•	11	Streetcar Dispatch	9:48:19 PM	
•	3	Incident 10	9:48:13 PM	
•	4	Streetcar Dispatch	9:48:12 PM	
•	3	Fire Main	9:48:11 PM	
▶	8	MPD Citywide	9:48:02 PM	
•	3	Unified Comm Center 3	9:47:59 PM	
•	0	Unified Comm Center 3	9:47:55 PM	
•	4	MPD Citywide	9:47:54 PM	
•	11	Streetcar Dispatch	9:47:53 PM	
•	4	Fire Main	9:47:51 PM	
•	5	Streetcar Dispatch	9:47:32 PM	
•	7	Incident 10	9:47:24 PM	
•	8	MPD Citywide	9:47:23 PM	
•	13	EMS 6	9:47:03 PM	★

MPD Citywide

1113970[0] • 116740[6.3]

SECONDS: 8
TALKGROUP: 1039

9:48:02 PM
1/11/2024
858.588 MHz

1Sec 1113970

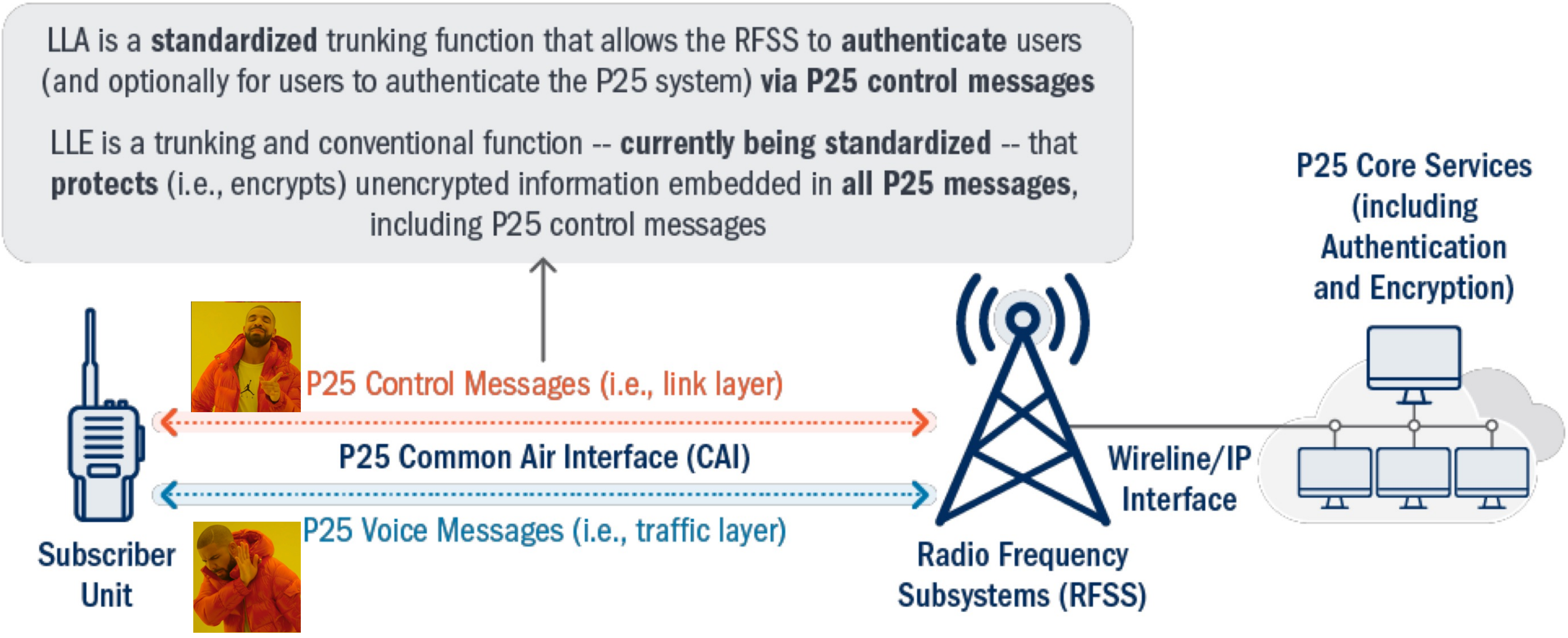
Share captured transmissions

- Community driven!
- *My other labor of Love*
- 30 day archive
- YOLO quality Web Service
- 220 Systems, mostly US
- Last 30 days:
  - 43,047,814 transmissions
  - 2.07 TB of compressed audio
- ~150k minutes of audio per day

NOW WITH APP!

P25 Traffic Analysis

Dot, Dash, Dash, Dot



LLA is a **standardized** trunking function that allows the RFSS to **authenticate** users (and optionally for users to authenticate the P25 system) **via P25 control messages**

LLE is a trunking and conventional function -- **currently being standardized** -- that **protects** (i.e., encrypts) unencrypted information embedded in **all P25 messages**, including P25 control messages

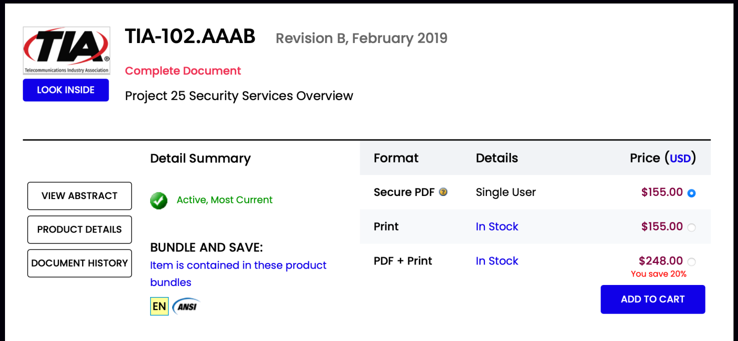
P25 Control Messages (i.e., link layer)
P25 Common Air Interface (CAI)
P25 Voice Messages (i.e., traffic layer)
Subscriber Unit
Radio Frequency Subsystems (RFSS)
Wireline/IP Interface
P25 Core Services (including Authentication and Encryption)

Figure 1. LLA and LLE Overview

https://www.cisa.gov/sites/default/files/2023-03/23_03.08_LLA_LLE_CLEAN_v2.pdf

P25 Encryption Standards

	Voice	Link Layer Authentication	Link Layer Encryption
Standardized	99ish?	2005	🙃
Widely Used	👍	👎	🤮



TIA-102.AAAB Revision B, February 2019

Complete Document

Project 25 Security Services Overview

Detail Summary

Active, Most Current

BUNDLE AND SAVE:
Item is contained in these product bundles

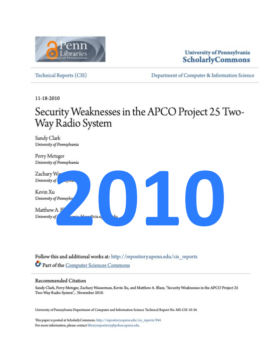
Format	Details	Price (USD)
Secure PDF	Single User	$155.00
Print	In Stock	$155.00
PDF + Print	In Stock	$248.00 You save 20%

OR....

INTERNET ARCHIVE

Search:
TIA-102_Series_Documents

Not Novel… *but Not Patched!*



University of Pennsylvania
ScholarlyCommons

Technical Reports (CIS) — Department of Computer & Information Science

11-18-2010

Security Weaknesses in the APCO Project 25 Two-Way Radio System

Sandy Clark
University of Pennsylvania

Perry Metzger
University of Pennsylvania

Zachary Wa[illegible]
University of [illegible]

Kevin Xu
University of Pennsylv[illegible]

Matthew A. B[illegible]
University of [illegible][illegible]blaze@cis.u[illegible]edu

Follow this and additional works at: http://repository.upenn.edu/cis_reports

Part of the Computer Sciences Commons

Recommended Citation

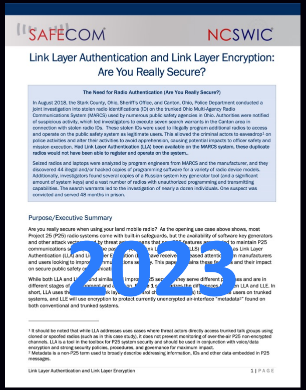
Sandy Clark, Perry Metzger, Zachary Wasserman, Kevin Xu, and Matthew A. Blaze, "Security Weaknesses in the APCO Project 25 Two-Way Radio System", . November 2010.

University of Pennsylvania Department of Computer and Information Science Technical Report No. MS-CIS-10-34.

This paper is posted at ScholarlyCommons. http://repository.upenn.edu/cis_reports/944
For more information, please contact libraryrepository@pobox.upenn.edu.

2010

Security Weaknesses in the APCO Project 25 Two-Way Radio System
Sandy Clark, Matt Blaze



SAFECOM NCSWIC

Link Layer Authentication and Link Layer Encryption: Are You Really Secure?

The Need for Radio Authentication (Are You Really Secure?)

In August 2018, the Stark County, Ohio, Sheriff's Office, and Canton, Ohio, Police Department conducted a joint investigation into stolen radio identifications (ID) on the trunked Ohio Multi-Agency Radio Communications System (MARCS) used by numerous public safety agencies in Ohio. Authorities were notified of suspicious activity, which led investigators to execute seven search warrants in the Canton area in connection with stolen radio IDs. These stolen IDs were used to illegally program additional radios to access and operate on the public safety system as legitimate users. This allowed the criminal actors to eavesdrop[1] on police activities and alter their activities to avoid apprehension, causing potential impacts to officer safety and mission execution. **Had Link Layer Authentication (LLA) been available on the MARCS system, these duplicate radios would not have been able to register and operate on the system..**

Seized radios and laptops were analyzed by program engineers from MARCS and the manufacturer, and they discovered 44 illegal and/or hacked copies of programming software for a variety of radio device models. Additionally, investigators found several copies of a Russian system key generator tool (and a significant amount of system keys) and a vast number of radios with unauthorized programming and transmitting capabilities. The search warrants led to the investigation of nearly a dozen individuals. One suspect was convicted and served 48 months in prison.

Purpose/Executive Summary

Are you really secure when using your land mobile radio? As the opening use case above shows, most Project 25 (P25) radio systems come with built-in safeguards, but the availability of software key generators and other attack vect[illegible] by threat act[illegible]eans that n[illegible] features ar[illegible]ed to maintain P25 communications s[illegible]he pas[illegible] ink L[illegible] (LLS) [illegible] as Link Layer Authentication (LLA) and Li[illegible]er E[illegible]tion (L[illegible] have receive[illegible]eased attentio[illegible]m manufacturers and users looking to impro[illegible]mmu[illegible]tions se[illegible]y. This pape[illegible]ains these fe[illegible]s and their impact on secure public safety c[illegible]nicati[illegible]

While both LLA and L[illegible]und simila[illegible] impro[illegible]25 sec[illegible]they serve different p[illegible]ses and are in different stages of [illegible]opment and a[illegible]ion. [illegible] 1 s[illegible]arizes the differences b[illegible]en LLA and LLE. In short, LLA uses th[illegible]nk lay[illegible]trol ch[illegible]s) to [illegible] users on trunked systems, and LLE will use encryption to protect currently unencrypted air-interface "metadata[2]" found on both conventional and trunked systems.

[1] It should be noted that while LLA addresses uses cases where threat actors directly access trunked talk groups using cloned or spoofed radios (such as in this case study), it does not prevent monitoring of over-the-air P25 non-encrypted channels. LLA is a tool in the toolbox for P25 system security and should be used in conjunction with voice/data encryption and strong security policies, procedures, and governance for maximum impact.

[2] Metadata is a non-P25 term used to broadly describe addressing information, IDs and other data embedded in P25 messages.

Link Layer Authentication and Link Layer Encryption 1 | PAGE

2023

Link Layer Authentication (LLA) and Link Layer Encryption (LLE): Are You Really Secure?
DHS Safecom

Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System

Sandy Clark Travis Goodspeed Perry Metzger Zachary Wasserman Kevin Xu Matt Blaze
University of Pennsylvania

APCO Project 25 ("P25") is a suite of wireless communications protocols used in the US and elsewhere for public safety two-way (voice) radio systems. The protocols include security options in which voice and data traffic can be cryptographically protected from eavesdropping. This paper analyzes the security of P25 systems against both passive and active adversaries. We found a number of protocol, implementation, and user interface weaknesses that routinely leak information to a passive eavesdropper or that permit highly efficient and difficult to detect active attacks. We introduce new *selective subframe jamming* attacks against P25, in which an active attacker with very modest resources can prevent specific kinds of traffic (such as encrypted messages) from being received, while emitting only a small fraction of the aggregate [illegible] legitimate [illegible]. We also found tha[illegible]e atta[illegible] present[illegible]erious practical threat. In a[illegible] we co[illegible]ed over [illegible] year period in several U[illegible]opoli[illegible]eas, we [illegible] that a significant fracti[illegible]he "en[illegible]ed" P25 [illegible]l radio traffic sent [illegible]eral law e[illegible]ement su[illegible]ance operatives is [illegible]y sent in th[illegible]r, in sp[illegible] their users' beli[illegible] they are encry[illegible] and o[illegible]eveals such sens[illegible]ames [illegible] criminal investigations.

1 Introduction

APCO Project 25 [16] (also called "P25") is a suite of digital protocols and standards designed for use in narrowband short-range (VHF and UHF) land-mobile wireless two-way communications systems. The system is intended primarily for use by public safety and other government users.

The P25 protocols are designed by an international consortium of vendors and users (centered in the United States), coordinated by the Association of Public Safety Communications Officers (APCO) and with its standards documents published by the Telecommunications Industry Association (TIA). Work on the protocols started in 1989, with new protocol features continuing to be refined and standardized on an ongoing basis.

The P25 protocols support both digital voice and low bit-rate data messaging, and are designed to operate in stand-alone short range "point-to-point" configurations or with the aid of infrastructure such as repeaters that can cover larger metropolitan and regional areas.

P25 supports a number of security features, including optional encryption of voice and data, based on either manual keying of mobile stations or "over the air" rekeying ("OTAR" [15]) through a key distribution center.

[illegible]is paper, we [illegible] the security of the P25 (a[illegible]mmon imp[illegible]s of it) against unauthorized [illegible]vesdropping, pas[illegible]nd active traffic analysis, an[illegible]ial-of-service thro[illegible]elective jamming.

[illegible] paper has three [illegible] contributions: First, we gi[illegible] (informal) analys[illegible]he P25 security protocols an[illegible]dard implementa[illegible]. We identify a number of [illegible]nd wea[illegible]curity properties of [illegible] agains[illegible]ries as well as ambiguities in the standard usage model and user interface that make ostensibly encrypted traffic vulnerable to unintended and undetected transmission of cleartext. We also discovered an implementation error, apparently common to virtually every current P25 product, that leaks station identification information in the clear even when in encrypted mode.

Next, we describe a range of practical active attacks against the P25 protocols that can selectively deny service or leak location information about users. In particular, we introduce a new active denial-of-service attack, *selective subframe jamming*, that requires *more than an*

2011

Why (Special Agent) Johnny (Still) Can't Encrypt
Sandy Clark, Matt Blaze

Recon Village

Nosy Cops: Exposing the Hidden Potential of Police Radio

sally, who makes yachts (@sally_yachts)

RECON VILLAGE

Nosy Cops: Exposing the Hidden Potential of Police Radio

SALLY, WHO MAKES YACHTS
@sally_yachts

11th Aug, 2023, Hotel Linq, Las Vegas.

16:30 PM to 17:10 PM

www.reconvillage.org

DEF CON 31
August 10-13, 2023
Las Vegas

0:02 / 42:32

DEF CON 31 Recon Village - Sally - Nosy Cops Exposing the Hidden Potential of Police Radio

Nosy Cops Exposing the Hidden Potential of Police Radio
@Sally_Yachts / DEFCON 31

P25 Control Channel Analysis

LOTS of interesting data on the Control Channel

Transmissions: Talkgroup and radio ID for each transmission

Registration: When every radio is turned on and off

- Radios are dedicated to vehicles and sometime to people

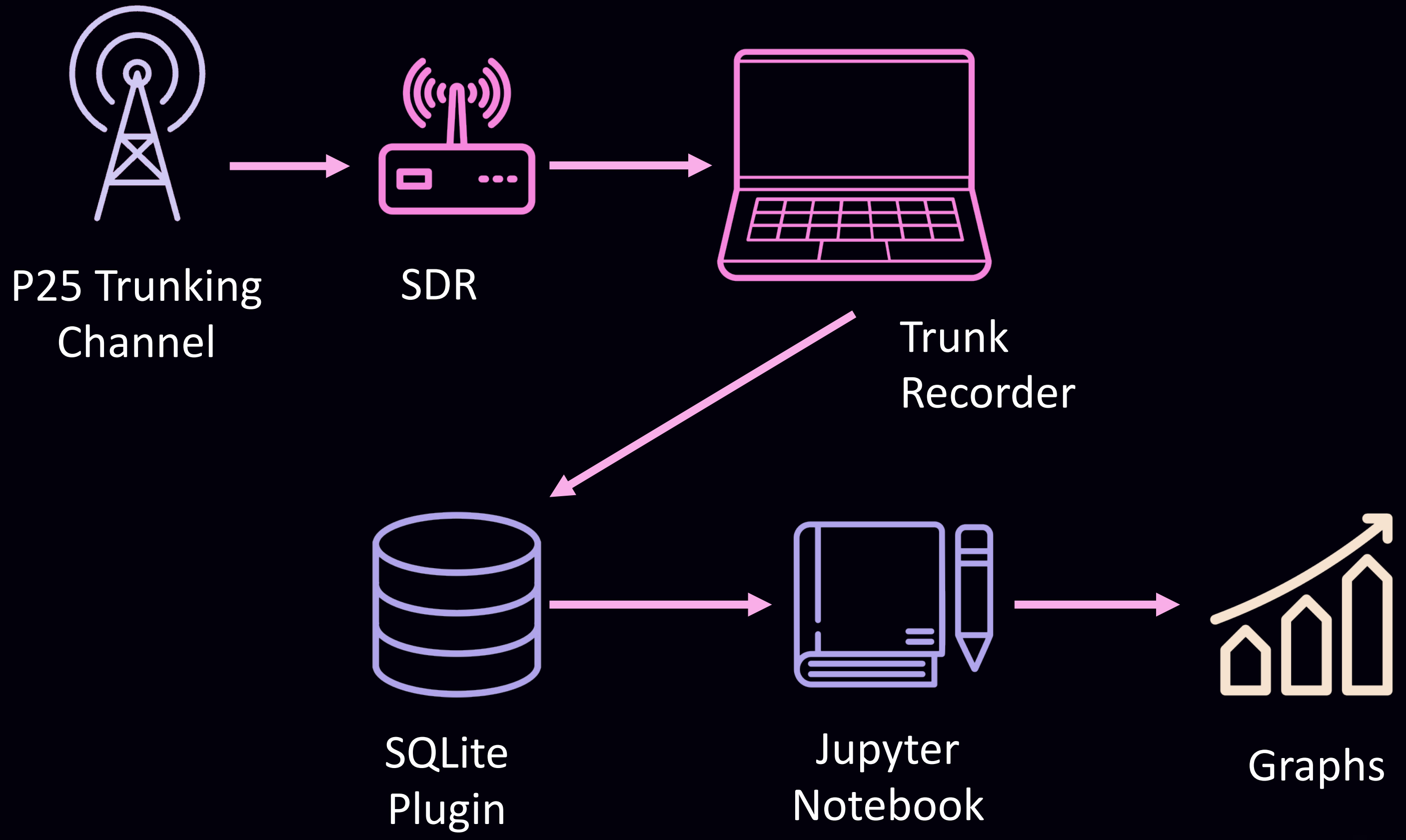
Affiliation: Each radio that is listening to a talkgroup

There are also **ACTIVE** things you can do...

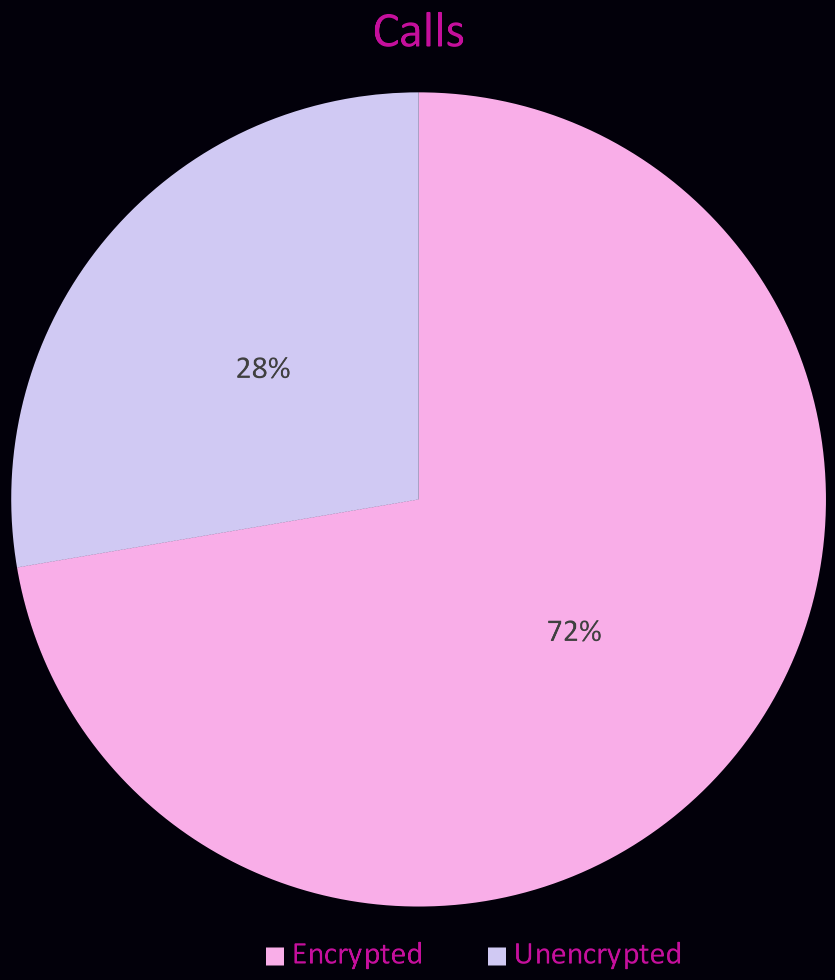
But we are not going there...

My Setup

JV Data Science



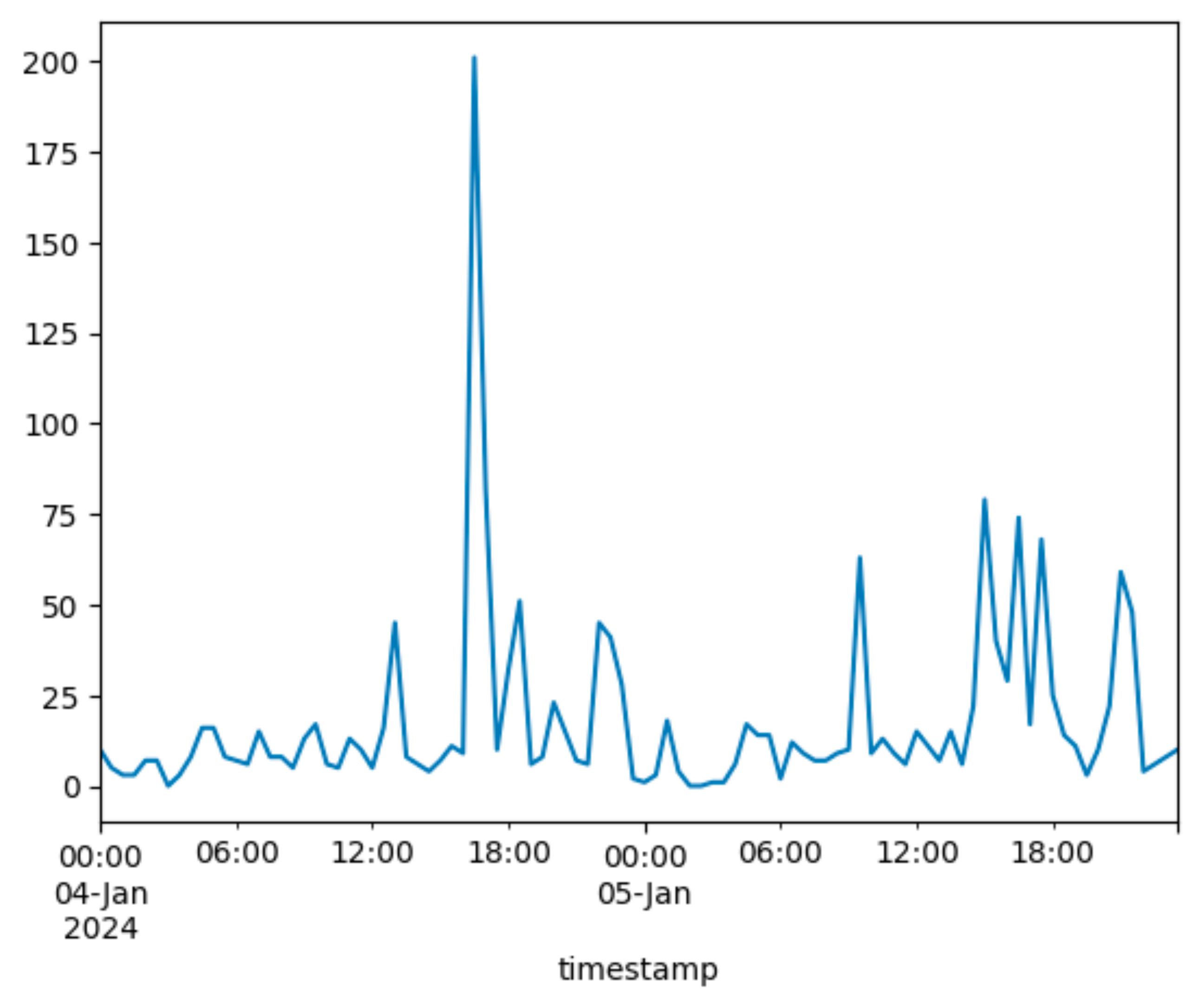
Lot’s of Encryption!

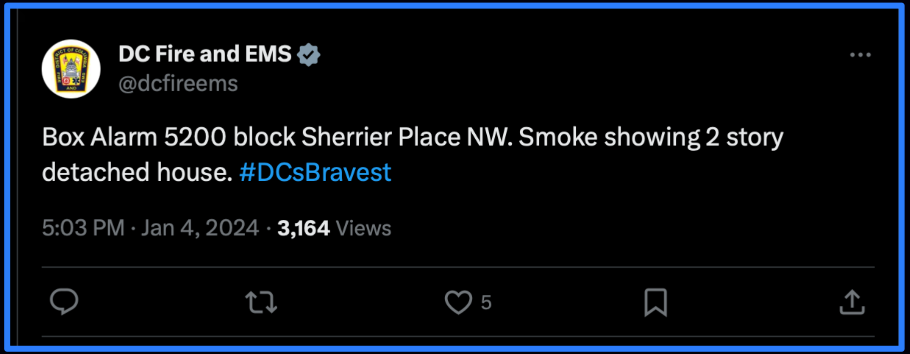


- ~9 Days
- 70,646 Unencrypted Calls
- 184,642 Encrytped Calls
- 255,288 Total Calls
- Generally…
  - Police = Encrypted
  - Fire/EMS = Unencrytped

Radio / TG Affiliation – In the Clear

TG 700 – Incident 10 – Radio Affiliation




DC Fire and EMS
@dcfireems

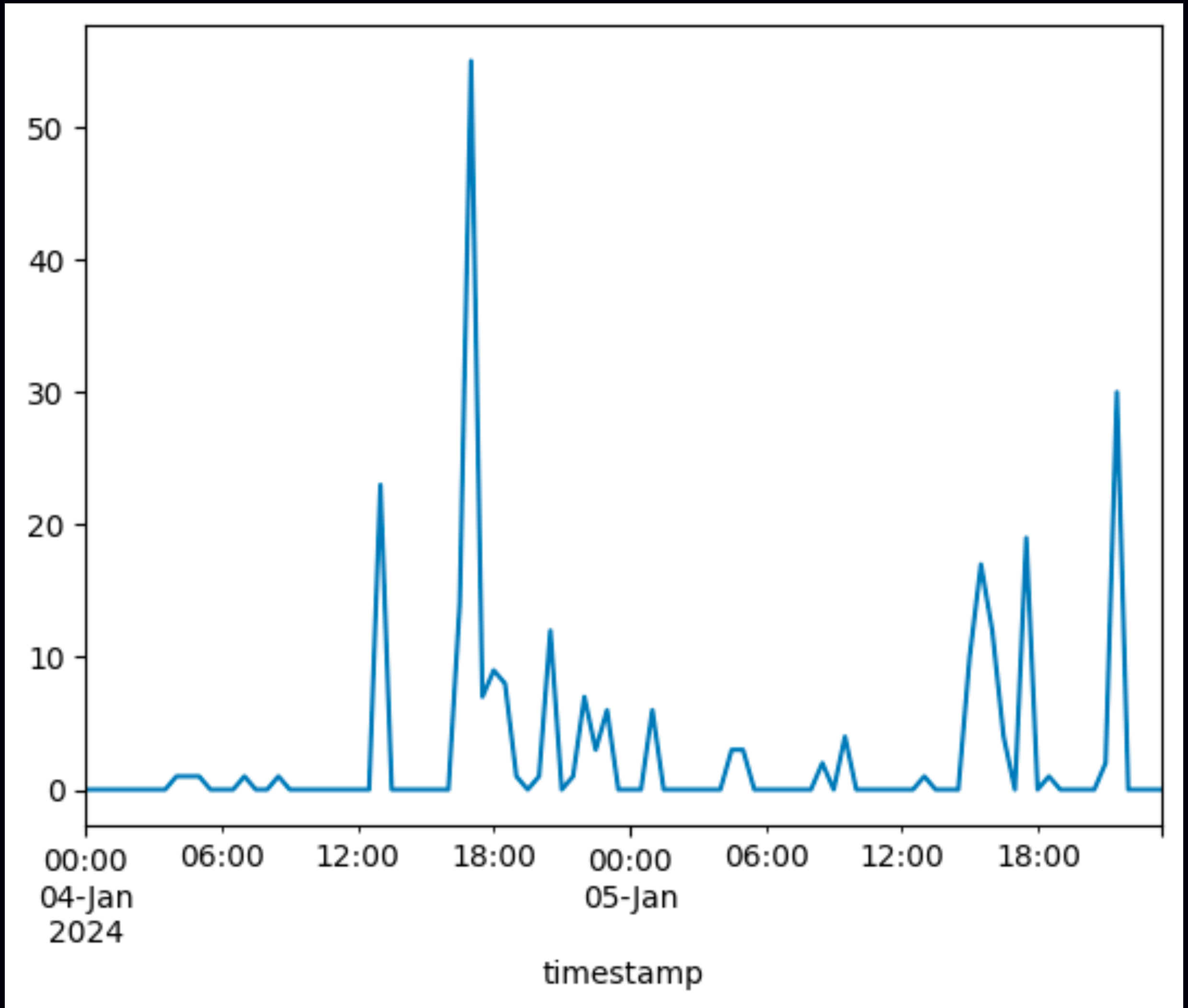
Box Alarm 5200 block Sherrier Place NW. Smoke showing 2 story detached house. #DCsBravest

5:03 PM · Jan 4, 2024 · **3,164** Views

- Counts Listners, not transmissions
- Everyone loves a Box Alarm

What did we learn?

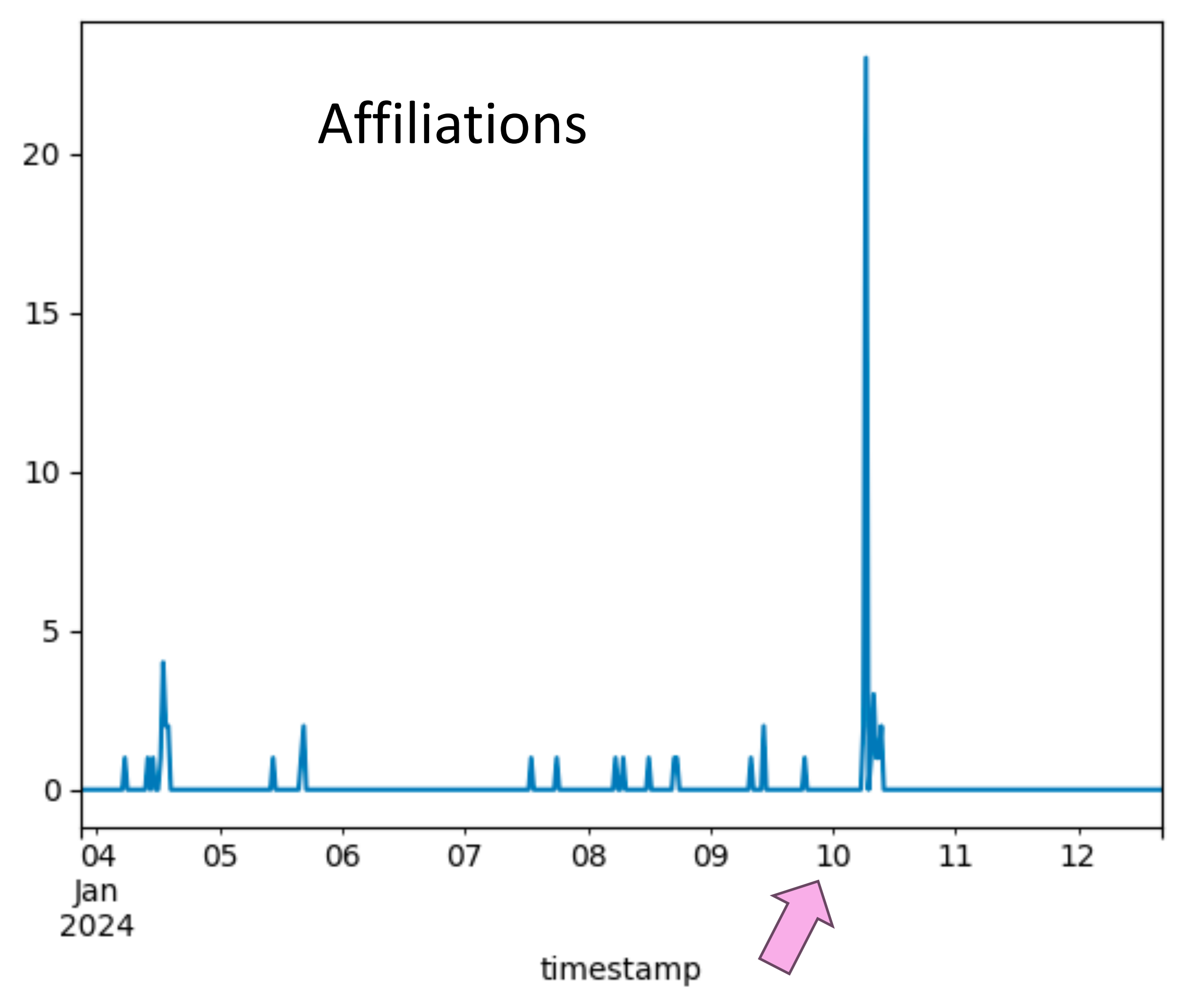
TG 700 – Incident 10 – Transmissions

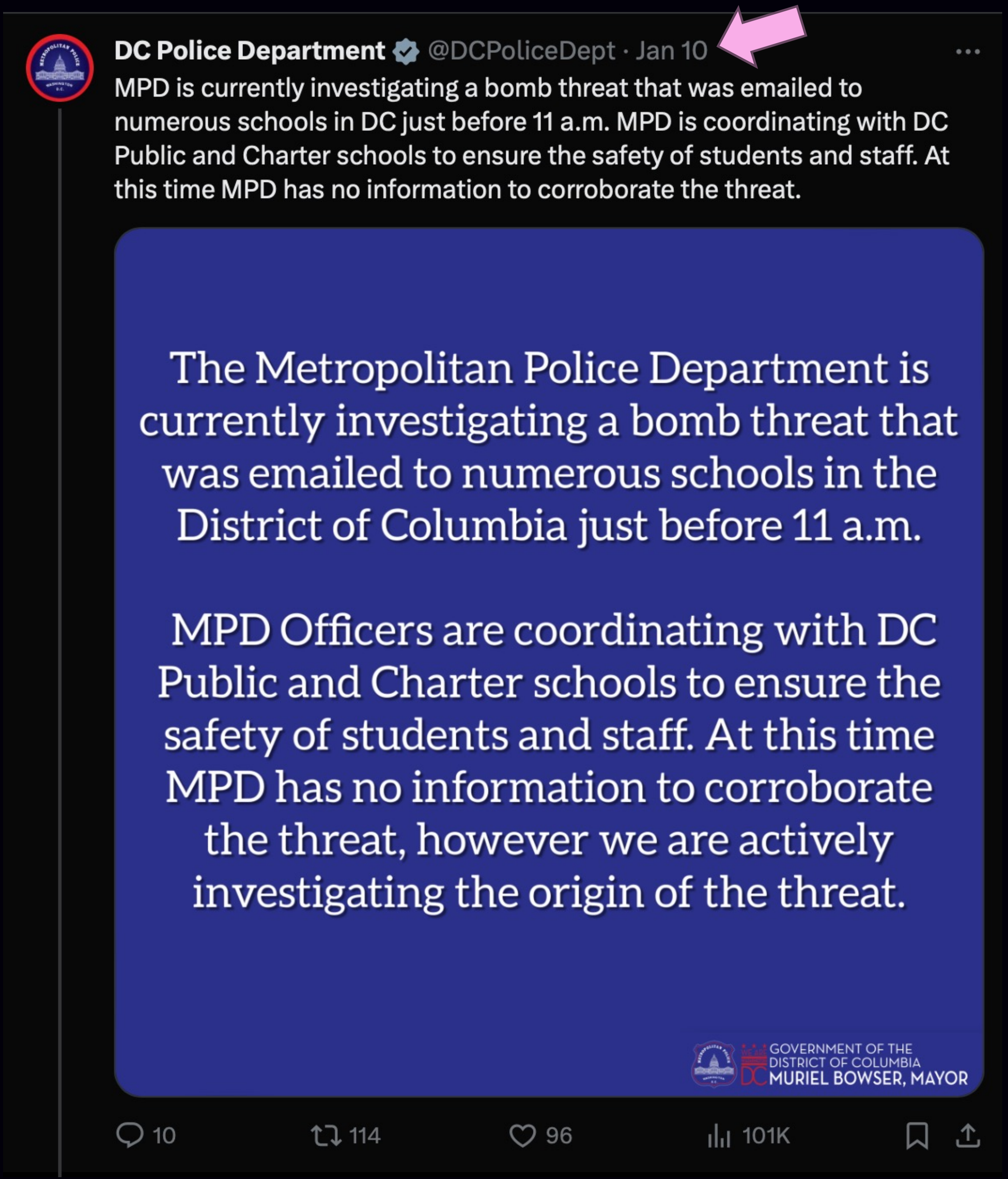


- Affiliation = Radio Units that are interested in Fireground
- Transmission = Radio Units that were active in Response
- Level of interest / activity – 4/1
- Duration of Activity

Let’s apply this…

TG 11151 – Special Operations Division 2 Emergency Response Team





DC Police Department @DCPoliceDept · Jan 10

MPD is currently investigating a bomb threat that was emailed to numerous schools in DC just before 11 a.m. MPD is coordinating with DC Public and Charter schools to ensure the safety of students and staff. At this time MPD has no information to corroborate the threat.

The Metropolitan Police Department is currently investigating a bomb threat that was emailed to numerous schools in the District of Columbia just before 11 a.m.

MPD Officers are coordinating with DC Public and Charter schools to ensure the safety of students and staff. At this time MPD has no information to corroborate the threat, however we are actively investigating the origin of the threat.

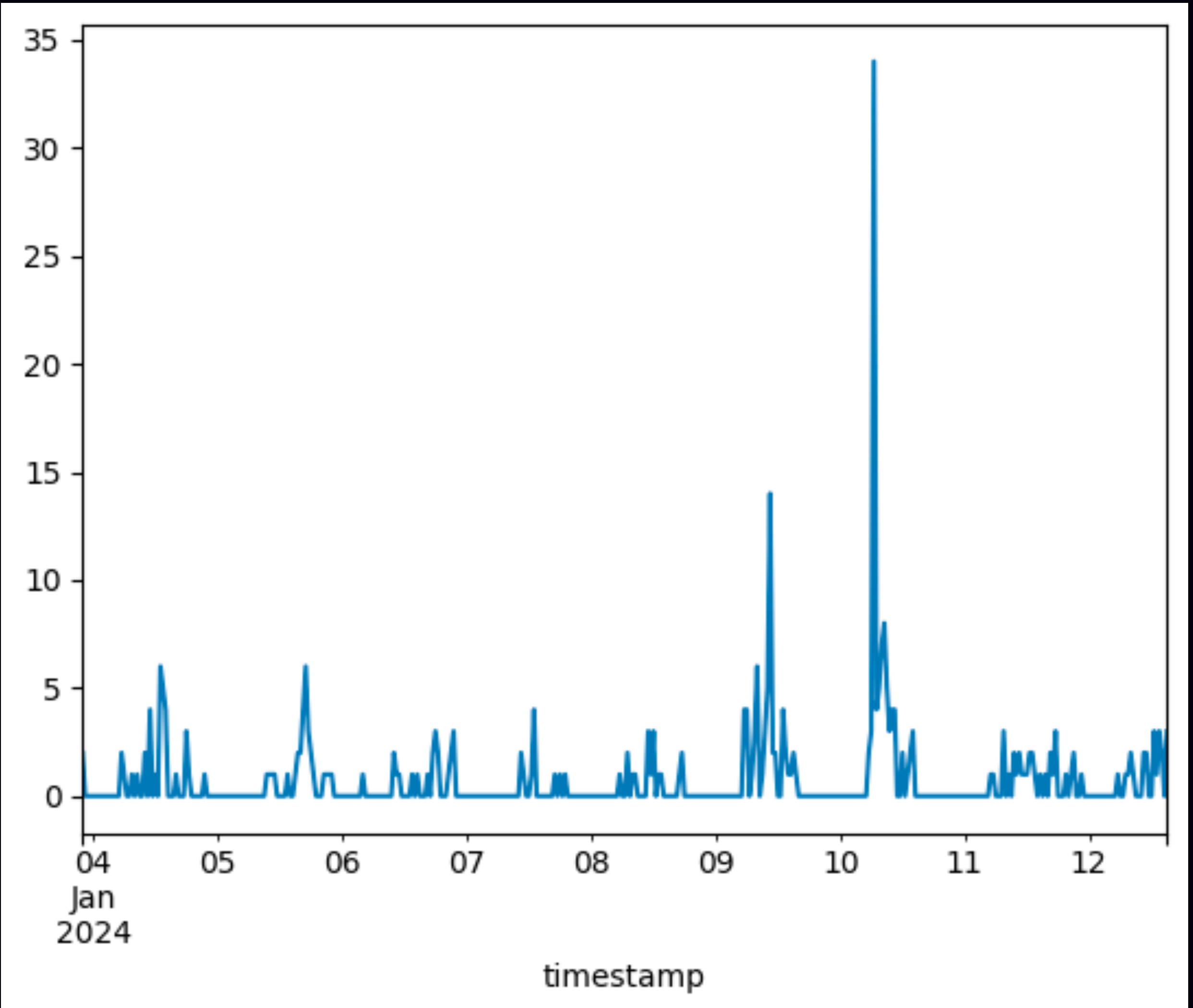
GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

Which Radios Tuned to TG 11151?

```
unit_list = [1102722, 1111218, 1111182, 1111150,
1102787, 1110846, 1111190, 1102736, 1103288, 1111116,
1102718, 1102766, 1102729, 1102695, 1102748, 1111195,
1102723, 1102685, 1110799, 1103692, 1102765, 1102728,
1102745, 1111253, 1102756, 1111368, 1102750, 1102727,
1267684, 1267746, 1102785, 1102651, 1102647, 1102784,
1102710, 1102783, 1102726, 1102780, 1102711, 1105798,
1111215, 1111494, 1110763, 1102713]
```

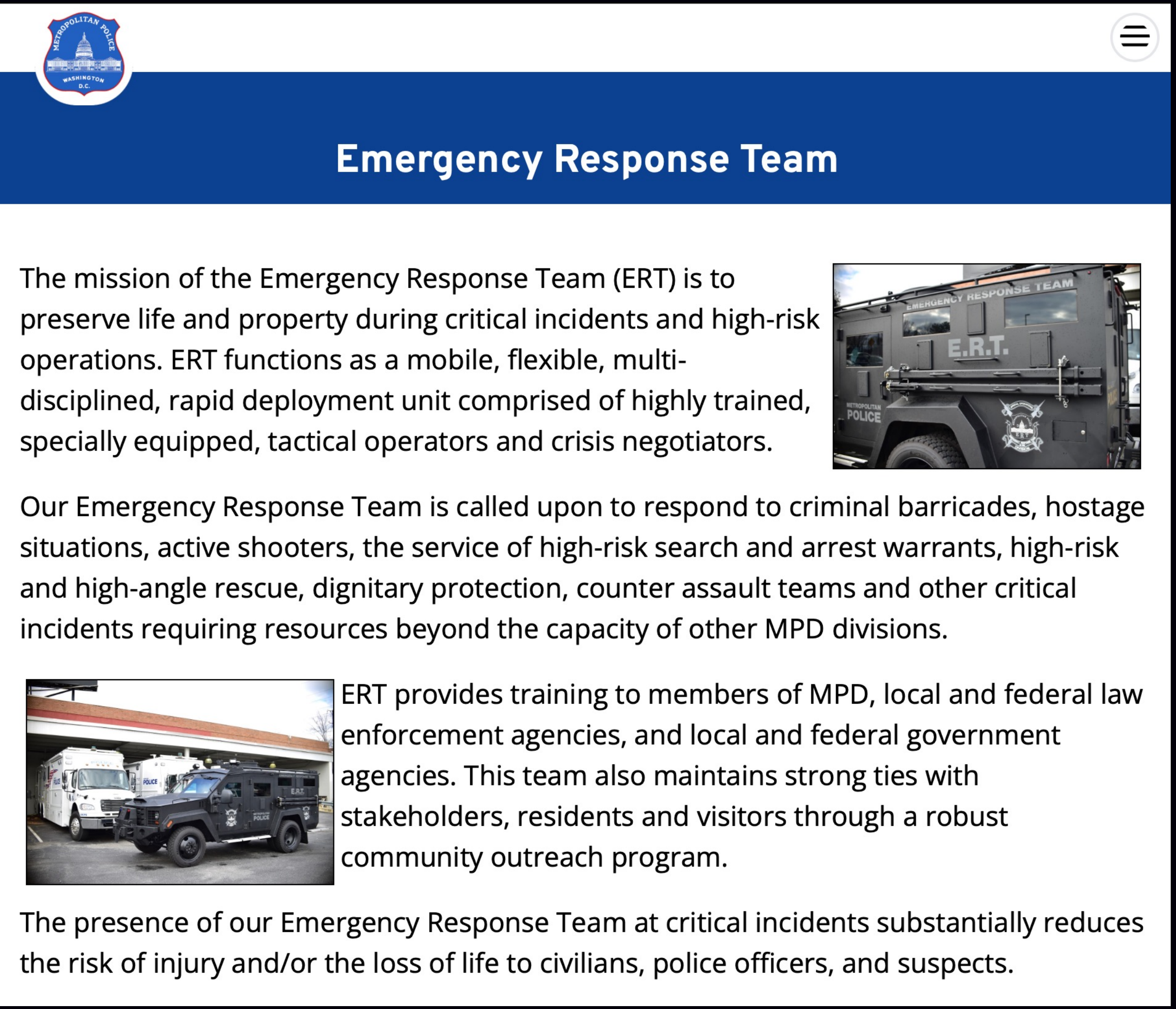
…and When are They Turned On?

`unit_list` Radio Registration



- Some of the radios are turned on regularly
- AND some seem to be only turned on when special things happen

Pure Speculation….



Emergency Response Team

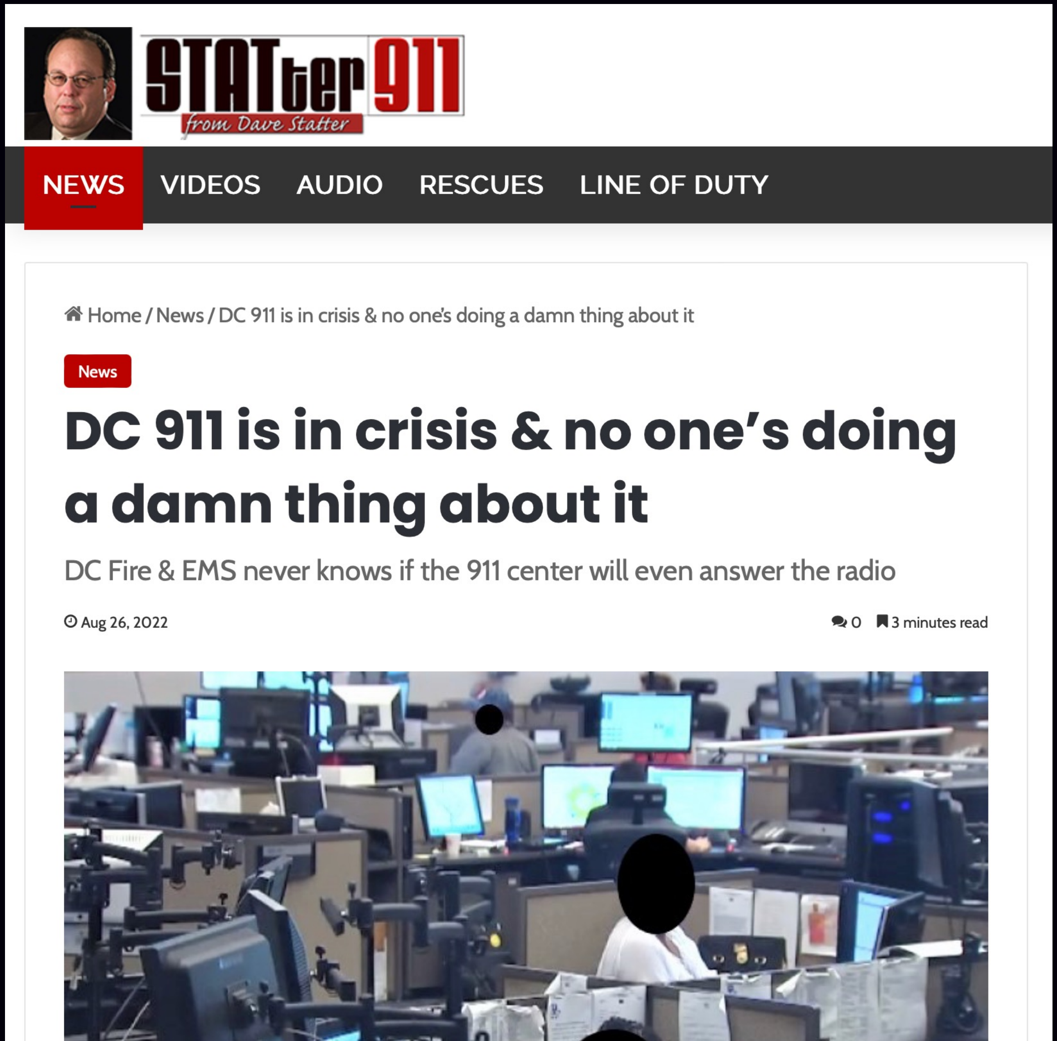
The mission of the Emergency Response Team (ERT) is to preserve life and property during critical incidents and high-risk operations. ERT functions as a mobile, flexible, multi-disciplined, rapid deployment unit comprised of highly trained, specially equipped, tactical operators and crisis negotiators.

Our Emergency Response Team is called upon to respond to criminal barricades, hostage situations, active shooters, the service of high-risk search and arrest warrants, high-risk and high-angle rescue, dignitary protection, counter assault teams and other critical incidents requiring resources beyond the capacity of other MPD divisions.

ERT provides training to members of MPD, local and federal law enforcement agencies, and local and federal government agencies. This team also maintains strong ties with stakeholders, residents and visitors through a robust community outreach program.

The presence of our Emergency Response Team at critical incidents substantially reduces the risk of injury and/or the loss of life to civilians, police officers, and suspects.

Why Transparency is Important



Home / News / DC 911 is in crisis & no one's doing a damn thing about it

News

DC 911 is in crisis & no one's doing a damn thing about it

DC Fire & EMS never knows if the 911 center will even answer the radio

Aug 26, 2022 0 3 minutes read

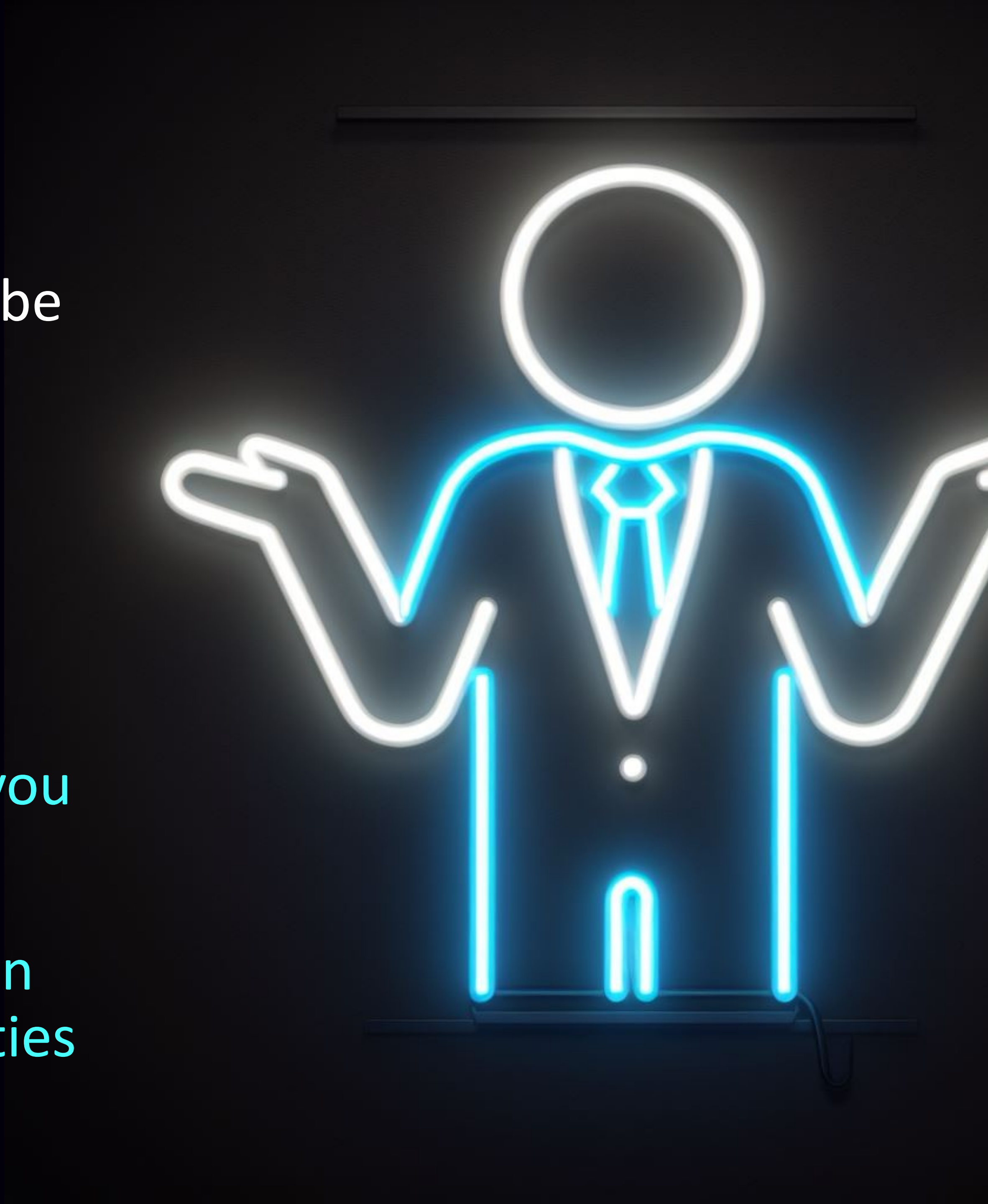
- DC's dispatch center is a disaster
- People have died because of their mistakes
- OpenMHz has helped discover and document these failures
- …but also all the issues around Police misconduct
- PLUS encryption makes interoperability tougher… inter-agency key sharing is tough

I am Conflicted

- I mean… it is a bad design that should be fixed and secured
- … but the openness can create trust in the community

Improve the design to make the things you are trying to secure… **secure**

Have a genuine community discussion on what should be open – balance of equities



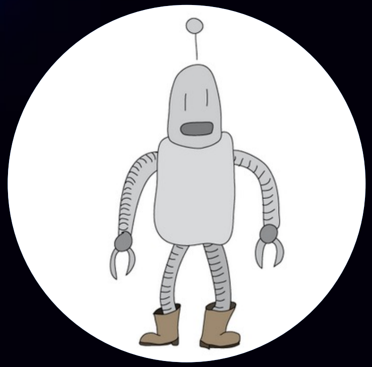
Research You Should DO!

- Cluster Radio IDs to the Talkgroups they listen to and talk on
- Track when particular radios turn on and off
  - Which are special units?
- Who talks when?
  - Chain of command
- Build an ‘oh shit’ alarm – Pi + 🚨 + SDR

Thank You!

Slides will be at:

lukeberndt.com



@lukeberndt
@robotastic
luke@robotastic.com