IOWA STATE UNIVERSITY

Department of Electrical and Computer Engineering

Cyber-Physical Attacks on Civil Defense Sirens

By: Ashler Benda, Michael Dorland, Tiffanie Fix

Outline

1 Introduction

2 Industry Leaders

3 Relevant Protocols

4 Issue Identified

5 Solutions Proposed

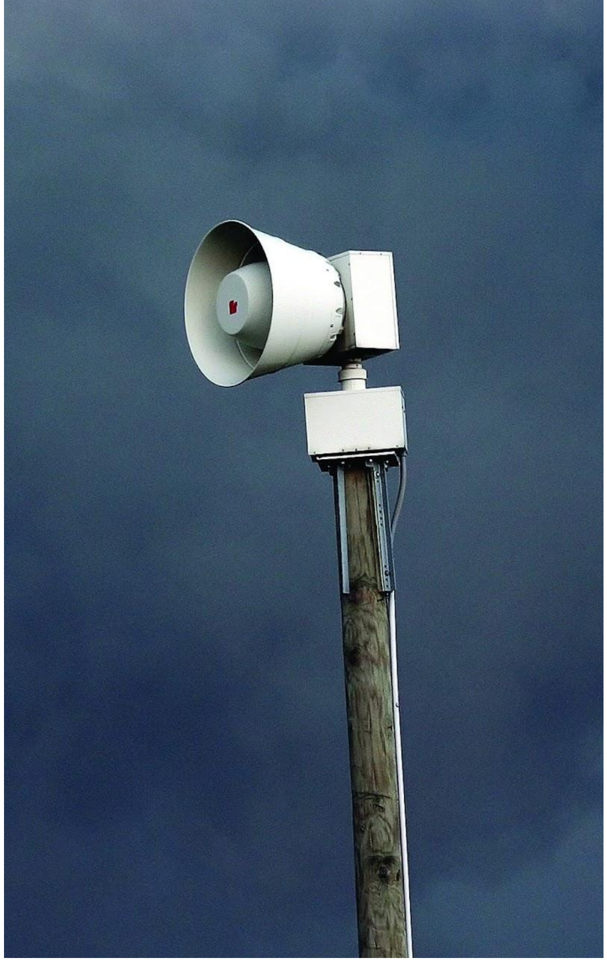
6 Conclusion

Introduction

Civil Defense Sirens and their Significance.

Background

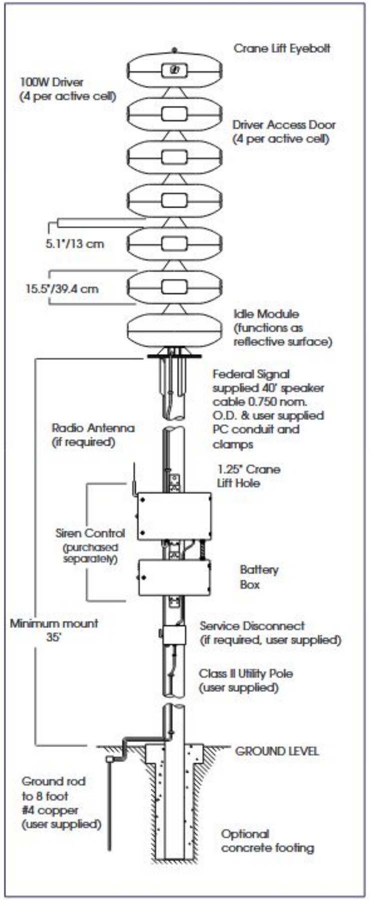
- Civil defense Sirens are an outdoor warning system used to alert the public mass of an immediate threat to human life
  - Also known as air-raid or tornado sirens
- Managed by local government and municipalities.



Siren Specifications

- Modern systems are electronic or electro-mechanical systems
  - Electro-mechanical can only disseminate sound
  - Electronic can disseminate sound and voice
- Activated by push-button or wireless technologies such as cellular, satellite, and radio
  - Some sirens support activation via the Common Alerting Protocol (CAP)
- Operates on signals within the range of 300-1000Hz
- Testing option include silent test and sound

MODULATOR® SPEAKER ARRAY (MOD)



Industry Leaders

Suppliers and Manufacturers of Sirens

Suppliers

- Civil Defense Sirens are not managed by federal government
  - Sirens are sold by suppliers
  - City is responsible for installation
- Manufacturers of these sirens are usually private sector.
  - Managing and operating sirens are considered public sector

Acoustic Technology Inc

- Solutions:
  - Outdoor
  - Mobile
  - Control
- Strictly Electromechanic products
- Notable customers:
  - NASA
  - US Air Force

ATI Systems
ACOUSTIC TECHNOLOGY, INC.

Federal Signal

- Leading producer of sirens in the U.S.
- Manufacture both electronic and electromechanical sirens
- Popular model include 2001 series, model 2, and Modulator 5020 (what campus uses)
- Solutions include radio, IP, landline, satellite and cellular

FEDERAL SIGNAL

Whelen Engineering

- Whelen offers electronic solutions
- Popular models include the WPS-2900 series, Vortex and Omni-One

WHELEN®

American Signal Corporation

- Electro-mechanical and mechanical sirens
- Popular model: Tempest series, I-Force, and E-Class
- Supplies: Government, Schools, Civilian

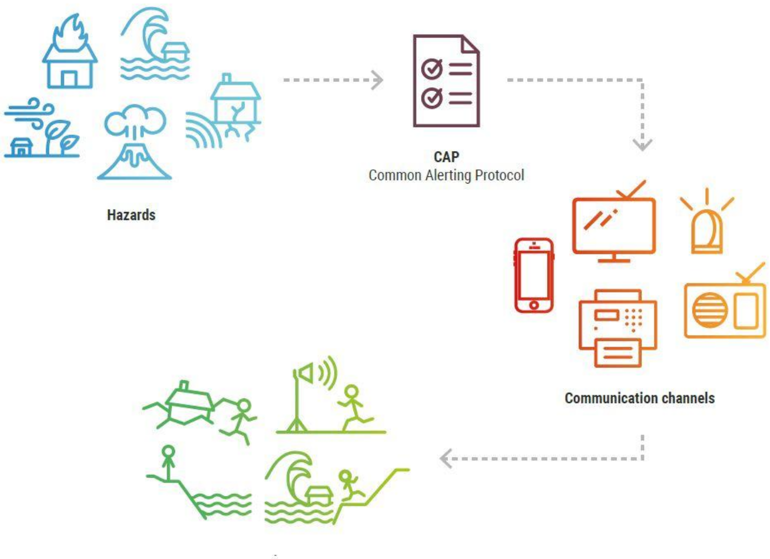
ASC
MASS NOTIFICATION SOLUTIONS

Relevant Protocols

Protocols used to Disseminate Information

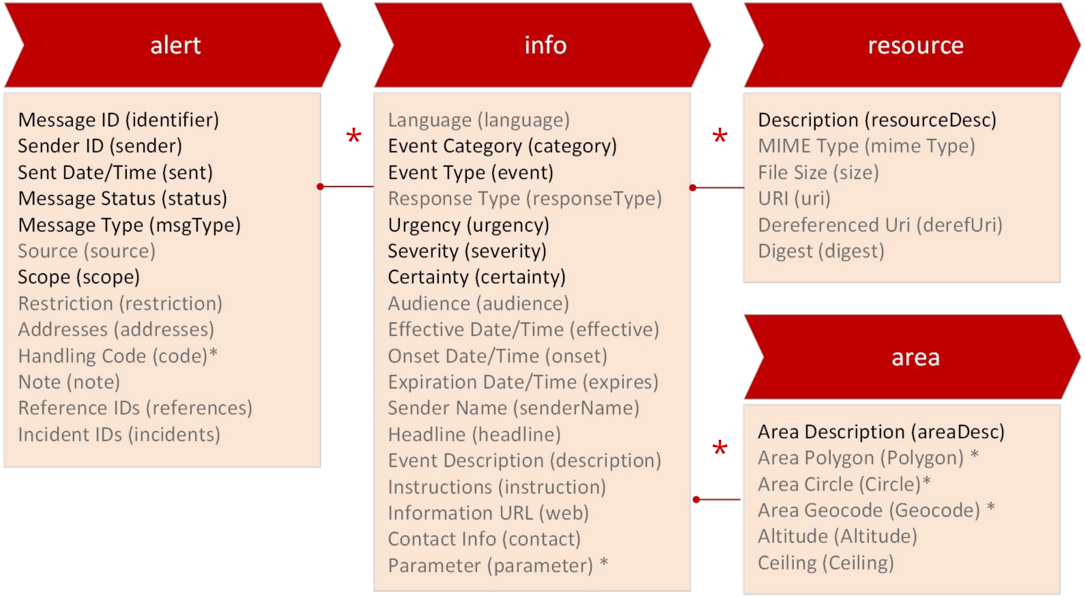
Common Alerting Protocol

- CAP is the format used for exchanging emergency alerts or public warning messages on a variety of platforms including cellular, radio, TV, and sirens.
- Adopted as a standard by the International Telecommunication Union (ITU)
- Used by sirens with CAP-enabled capabilities



Structure of a CAP message

- CAP message consists of segments <alert> ,<info>,<area> and/or <resource> segments.
- Each segment hold elements and sub-elements of information reporting the nature of the event
  - Within this figure black is required and gray is optional, * means multiple instances are allowed



alert

Message ID (identifier)
Sender ID (sender)
Sent Date/Time (sent)
Message Status (status)
Message Type (msgType)
Source (source)
Scope (scope)
Restriction (restriction)
Addresses (addresses)
Handling Code (code)*
Note (note)
Reference IDs (references)
Incident IDs (incidents)

*

info

Language (language)
Event Category (category)
Event Type (event)
Response Type (responseType)
Urgency (urgency)
Severity (severity)
Certainty (certainty)
Audience (audience)
Effective Date/Time (effective)
Onset Date/Time (onset)
Expiration Date/Time (expires)
Sender Name (senderName)
Headline (headline)
Event Description (description)
Instructions (instruction)
Information URL (web)
Contact Info (contact)
Parameter (parameter) *

*

resource

Description (resourceDesc)
MIME Type (mime Type)
File Size (size)
URI (uri)
Dereferenced Uri (derefUri)
Digest (digest)

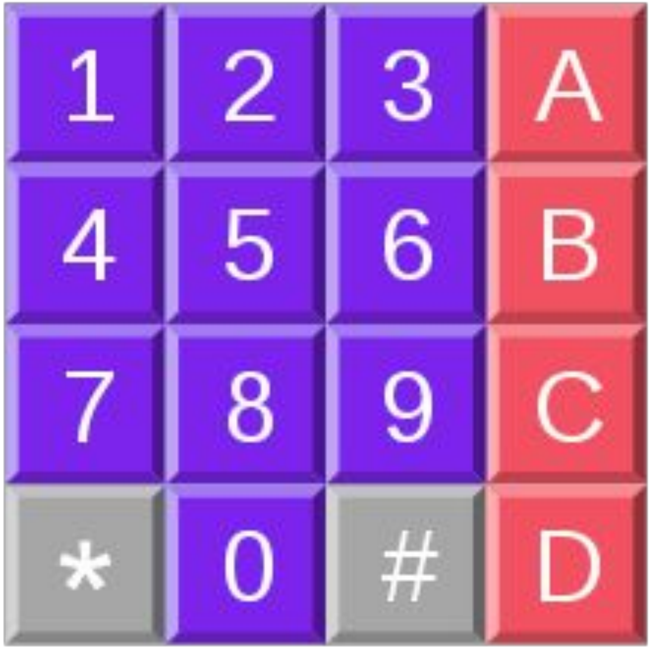
*

area

Area Description (areaDesc)
Area Polygon (Polygon) *
Area Circle (Circle)*
Area Geocode (Geocode) *
Altitude (Altitude)
Ceiling (Ceiling)

DTMF Encoding

- Commonly used for two way radio communication
- 16 Distinct Signals
- Location and functionally specific activation codes used to activate and test sirens



1	2	3	A
4	5	6	B
7	8	9	C
*	0	#	D

Issues Identified

The Dangers of Exploits Found within Sirens.

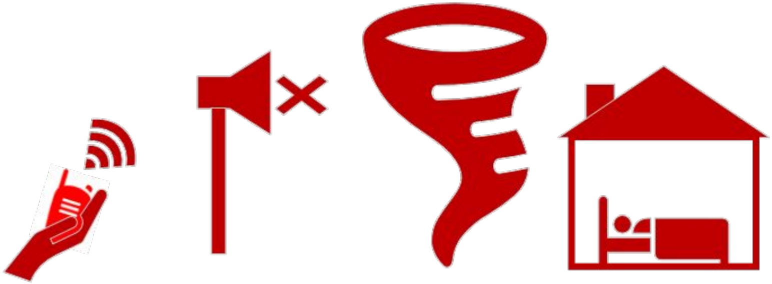
Problem Statement

- Siren technology must consider security while remaining reliable and accessible.
- Phasing out older sirens is expensive. Security patches are necessary
  - Cities often have a mix of digital and analog activated systems.

WARNING SIRENS HACKED
@FOX4
6:08
71°
SEVERE WEATHER SLOWS DOWN EFFORTS
TO FIX SIREN SYSTEM AFTER IT WAS HACKED

Risk Assessment

- Any exploit of this system carries a potential threat to human life and/or wellbeing.



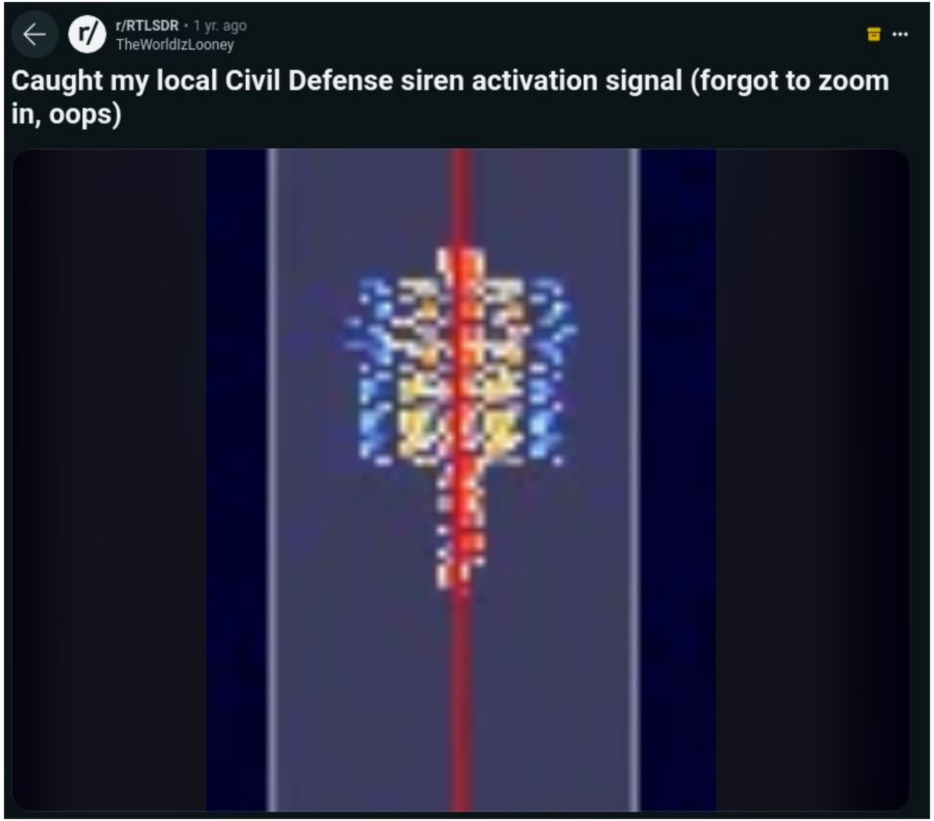
An adversary could attempt to jam the signal to prevent the public from being aware of an emergency.

The sirens could be activated outside of an actual emergency to cause a mass panic or public nuisance.

Replay Attack

Adversary just needs to identify the operational frequency band

Visual representation of DTMF encoded characters

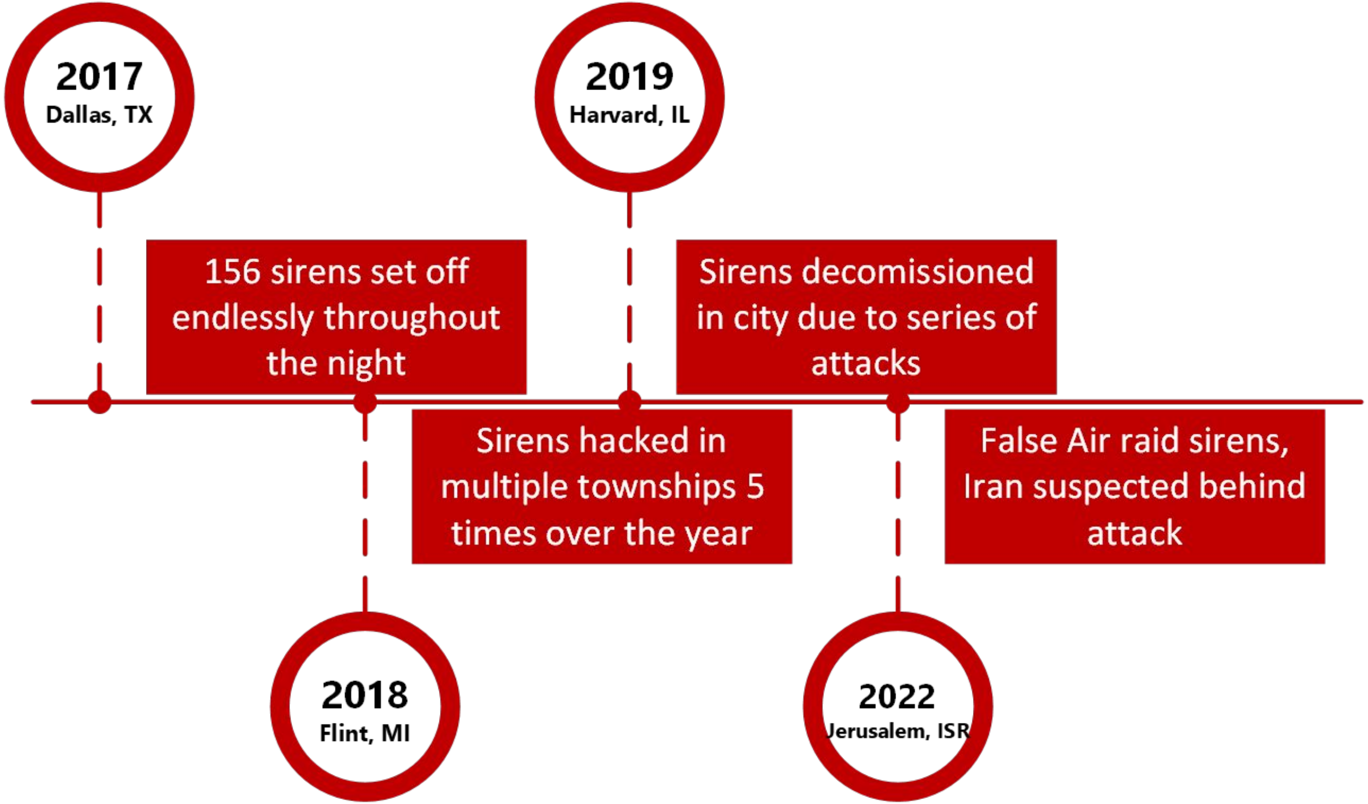


r/RTLSDR • 1 yr. ago
TheWorldIzLooney

Caught my local Civil Defense siren activation signal (forgot to zoom in, oops)

Demonstration

Real Life Cases



2017
Dallas, TX

156 sirens set off endlessly throughout the night

2018
Flint, MI

Sirens hacked in multiple townships 5 times over the year

2019
Harvard, IL

Sirens decomissioned in city due to series of attacks

2022
Jerusalem, ISR

False Air raid sirens, Iran suspected behind attack

Solution Proposed

Methods and Current Efforts in Mitigation.

Dallas Patch

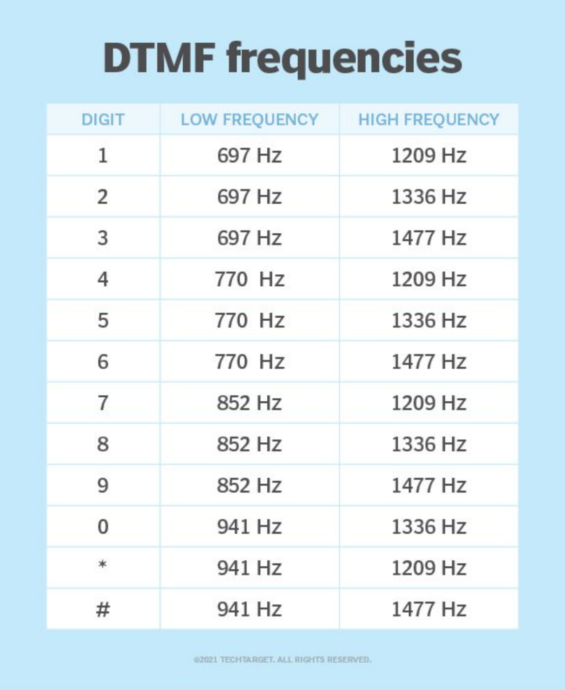
- Federal Signal systems
- Local attack, not remote access vulnerability
- Believed to be an attack taking advantage of weak encryption
- Radio based attack
- “fixed” by the vendor “West Shore Services”

ATI Patch

- Addressed:
    - Improper Authentication CVE-2018-8862
    - Lack of encryption CVE-2018-8864
- The patch “adds additional security features to the command packets sent over the radio”

DTMF Problems

- Easily intercepted by anyone listening on the frequency
- Conversion to back to numbers is easy
- Governing Body attitudes
- Security options
  - Switch to digital systems



DTMF frequencies

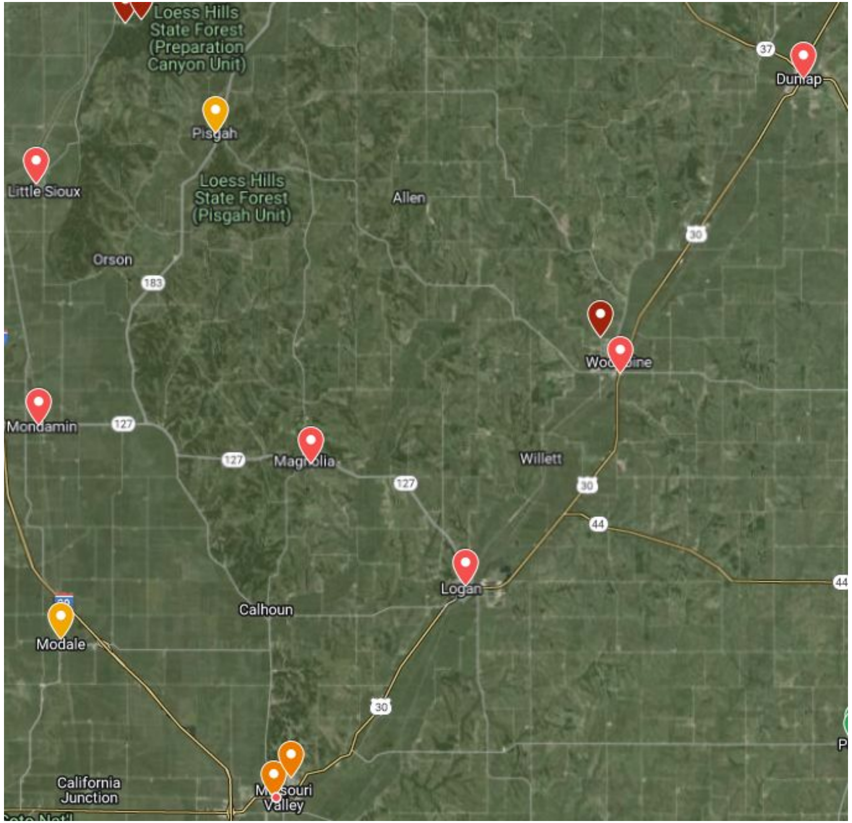
DIGIT	LOW FREQUENCY	HIGH FREQUENCY
1	697 Hz	1209 Hz
2	697 Hz	1336 Hz
3	697 Hz	1477 Hz
4	770 Hz	1209 Hz
5	770 Hz	1336 Hz
6	770 Hz	1477 Hz
7	852 Hz	1209 Hz
8	852 Hz	1336 Hz
9	852 Hz	1477 Hz
0	941 Hz	1336 Hz
*	941 Hz	1209 Hz
#	941 Hz	1477 Hz

DTMF Masking

- Tone Masking
  - Tones are replaced with a random tone or flat tone to hide the transmission
  - also known as “clamping”
  - eavesdroppers would only hear flat tones or the “asterisk” tone
  - Tones should not be linked to the masked tone.
  - Same tone for all or randomized

UPGRADES

- Replace with digital P-25 (APCO) radios
- Use CAPS protocol
- Remove unsecured DTMF options
- Look at your local sirens and ask questions



Best Practices

- Regular Patching
- User Access
- Passwords
- Inspections
- Integrity
- Physical Security
- Firewalls

Conclusion

Closing Observations

Being Vigilant

- Replace the old radio systems with digital networked ones
- Sirens **are** a target. Especially older systems. These are low-hanging fruit
- Change default passwords..
- Follow best practices issued by the Communications Security, Reliability, and Interoperability Council

Questions?