CUTAWAY SECURITY

INFOSEC CONSULTANTS

Detecting Encrypted Radio Communications Using Universal Radio Hacker

Don C. Weber - @cutaway

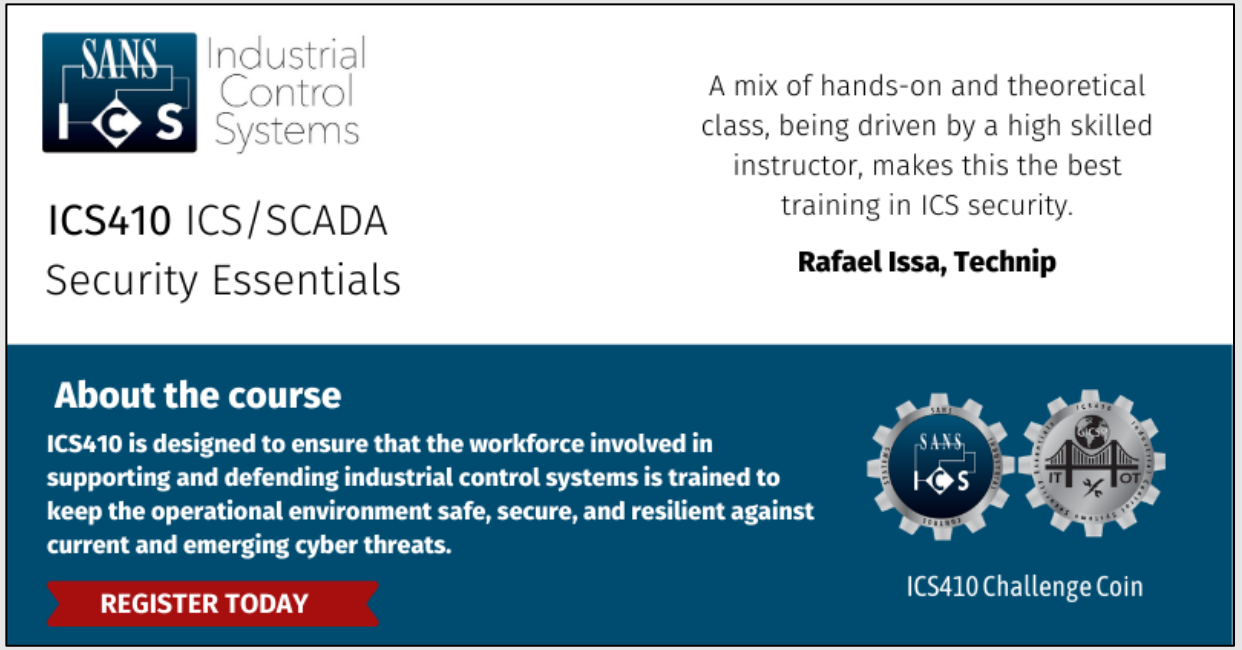
Principal Consultant, Founder

Presented at Wild West Hacking Fest 2020 on September 25, 2020

Cutaway Security, LLC / Don C. Weber

- ICS Security Assessments
- Penetration Testing
- Security Research

Special Thanks



Disclaimer

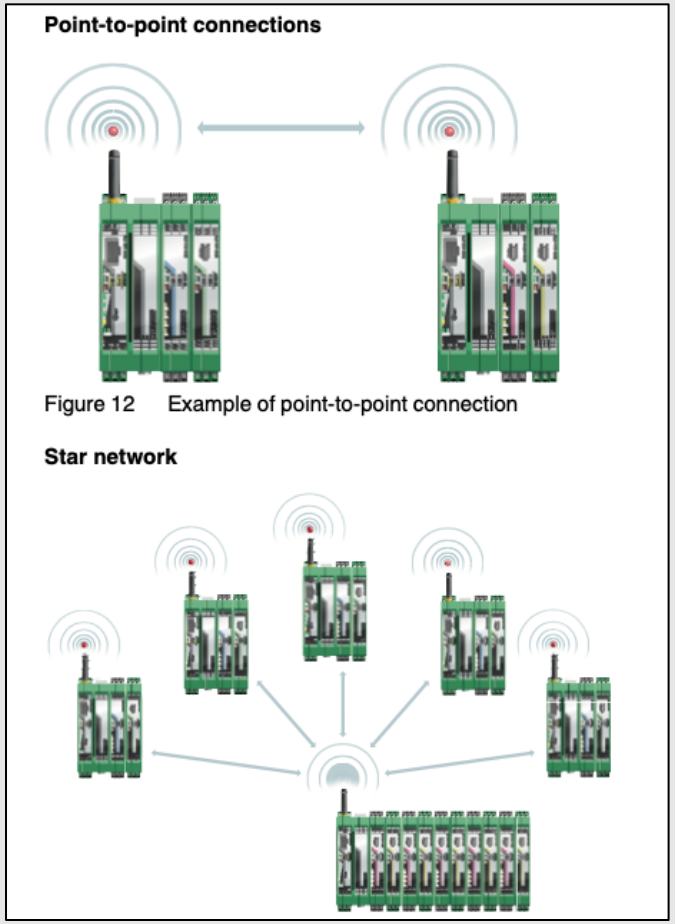
Images and references within the presentation, unless specifically identified, are not meant to imply vulnerabilities in the vendor's solution. Proper implementation is typically, depending on the vendor, located in the solution's implementation guides.

Please read these guides and outline security requirements during the planning phases and integrate into factory and site acceptance testing.

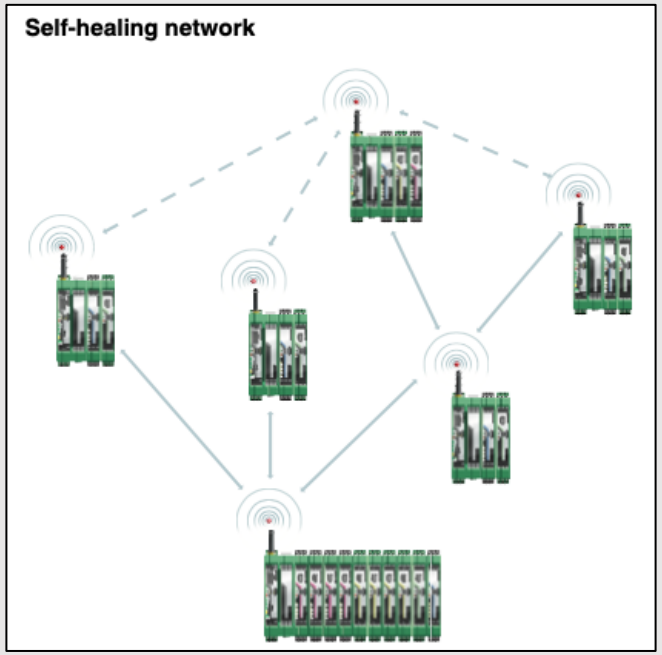
iMovie: Analyzing Radio Transmissions Using URH

https://www.cutawaysecurity.com/wp-content/uploads/2020/09/CutSec_WWHF_URH_HowTo2.mp4

Why are we here?



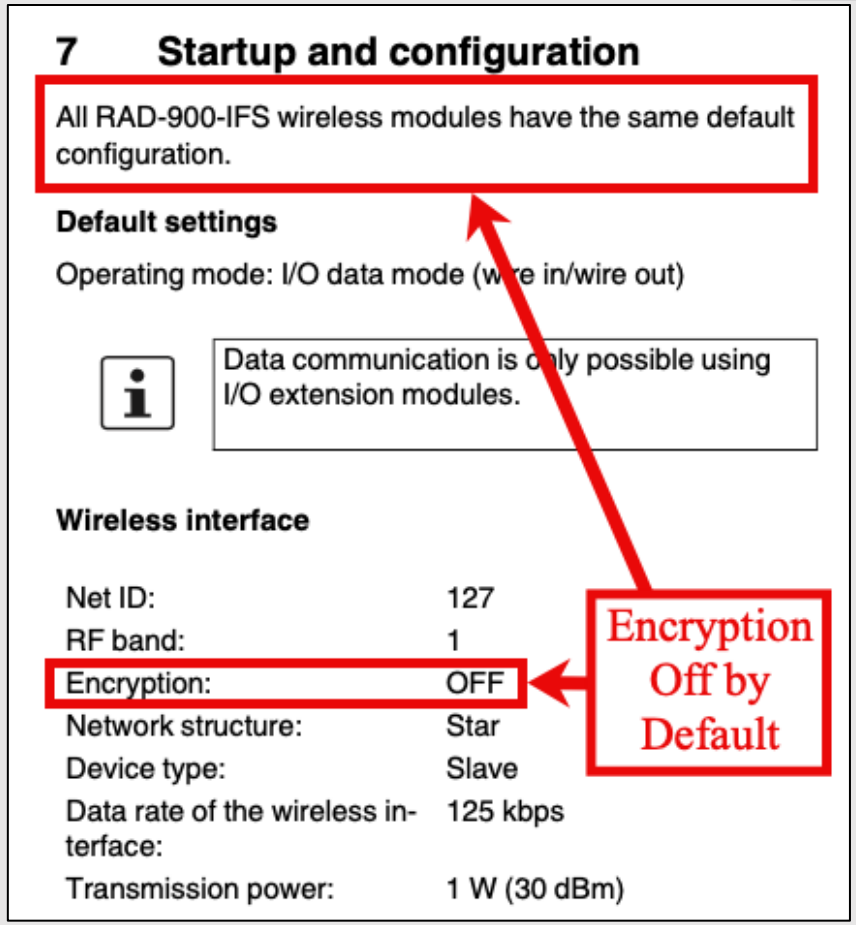
- Radio gateways and end-points provide connectivity where wires cannot be used.
- Radio enabled end-points monitor and control the process.
- Radios will always receive, and attempt to process, any data (malicious or otherwise) sent to it.



Source: Phoenix Contact RAD-900 User Manual
https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2702877&library=usen&tab=1

Wireless Solutions Provide Encryption

Wireless communication is based on Trusted Wireless 2.0 technology. The high demand for a interference-free data transmission using the license-free 900 MHz band, in particular via the use of the FHSS method (FHSS) and 128-bit data encryption (AES), is fulfilled.



7 Startup and configuration

All RAD-900-IFS wireless modules have the same default configuration.

Default settings

Operating mode: I/O data mode (wire in/wire out)

Data communication is only possible using I/O extension modules.

Wireless interface

Net ID:	127
RF band:	1
Encryption:	OFF
Network structure:	Star
Device type:	Slave
Data rate of the wireless interface:	125 kbps
Transmission power:	1 W (30 dBm)

Source: Phoenix Contact RAD-900 User Manual
https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2702877&library=usen&tab=1

Three Eternal Truths of Wireless Security + 1

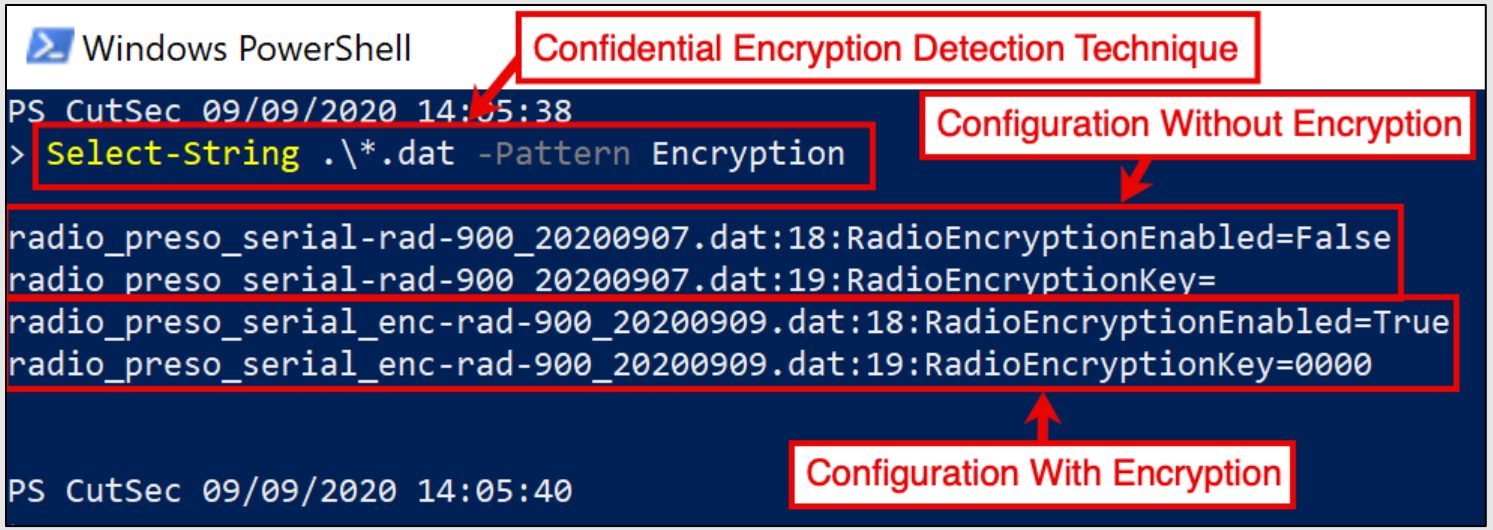
- Denial-of-Service attacks are easier and near impossible to defend against
- Network capture is possible, regardless of frequency or hopping techniques
- Attacker has at least a limited ability to communicate on the wireless network

- "When utilizing industrial wireless for a communication path in a process, ensure the process is designed and engineered to operate safely and reliably without that communication." – Tim Conway, The SANS Institute

Source: SANS ICS410 ICS / SCADA Security Essentials
https://www.sans.org/course/ics-scada-cyber-security-essentials

Radio Security Assessment Methodology

1. Obtain managing radio configuration file. *
2. Grep 'Encryption' **
3. Note results ***
4. ???? ****
5. Profit



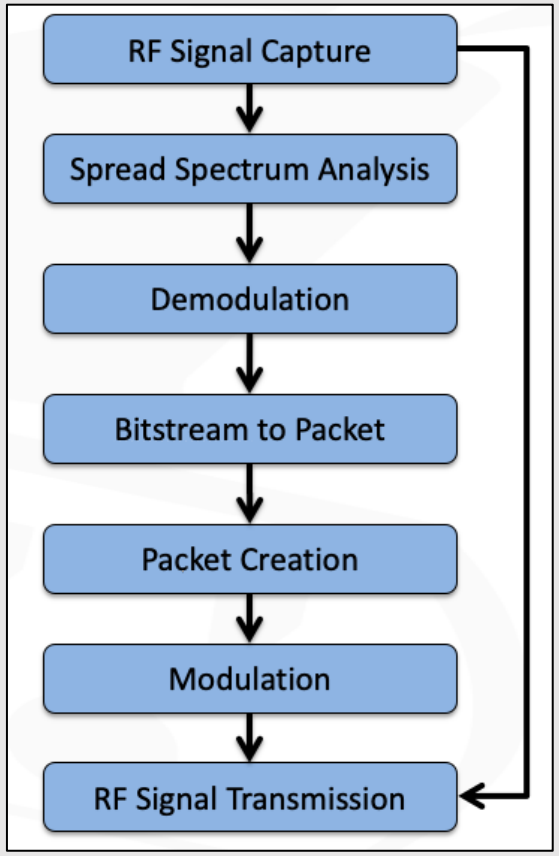
* Phoenix Contact RAD-900-IFS, in this example

** You'll be on Windows, so `Select-String .\ -Pattern Encryption`

*** Mitigate here, if these are your radios. If not, note "Key" value.

**** ???? is shorthand for Report / Document

Active Wireless Radio Assessment Methodology

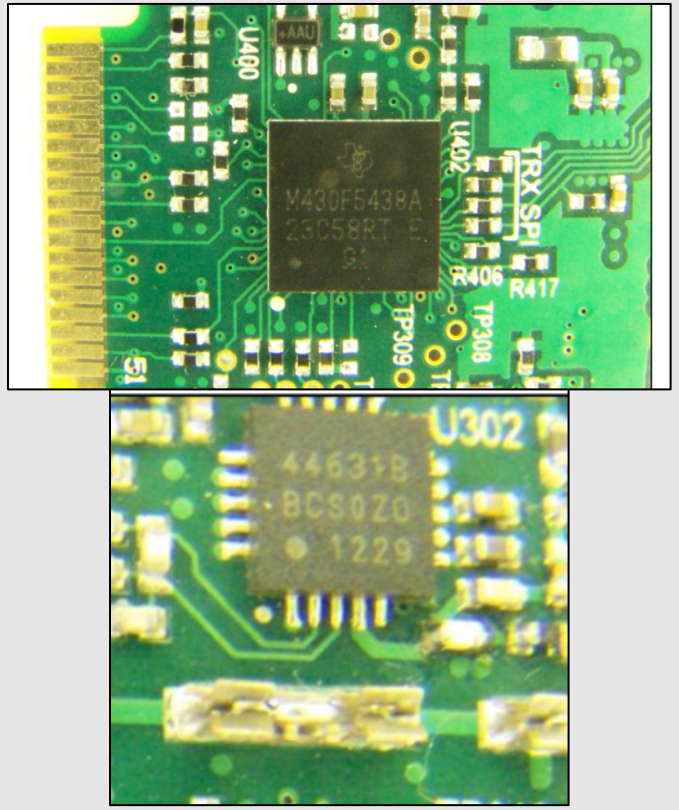


Source: ControlThings.io Accessing and Exploiting Control Systems
https://www.controlthings.io/training

- Research the target
- Determine best hardware and software equipment
- Setup lab with simulated targets
- Transmit, Capture, Analyze
- Transmit, Capture, Analyze
- Transmit, Capture, Analyze
- Transmit, Capture, Analyze…

Recon: Phoenix Contact RAD-900-IFS

- FCC ID: SGV-SHR-900
  - Product data from website (references on last slide)
- Radio: Silicon Labs (SI) 4431B
  - FCC Documents
- Frequency: 902 MHz – 928 MHz ISM band
  - Product data from website
- Spread Spectrum: Frequency Hopping
  - RAD-900-IFS Product datasheet
- Modulation: (G)FSK,4(G)FSK,(G)MSK,OOK
  - SI 4463B datasheet
- Preamble Byte: 10101010
  - SI 4463B datasheet
  - Length: 4 (typical default, from experience)
- Sync Word: 0xB42B
  - SI Packet Handler Operation For Si446x RFICs datasheet
- Cyclical Redundancy Check: X15+X12+X5+1 16-bit polynomial
  - Example code from SI Packet Handler Operation For Si446x RFICs datasheet



Source: RAD-900 FCC Documentation

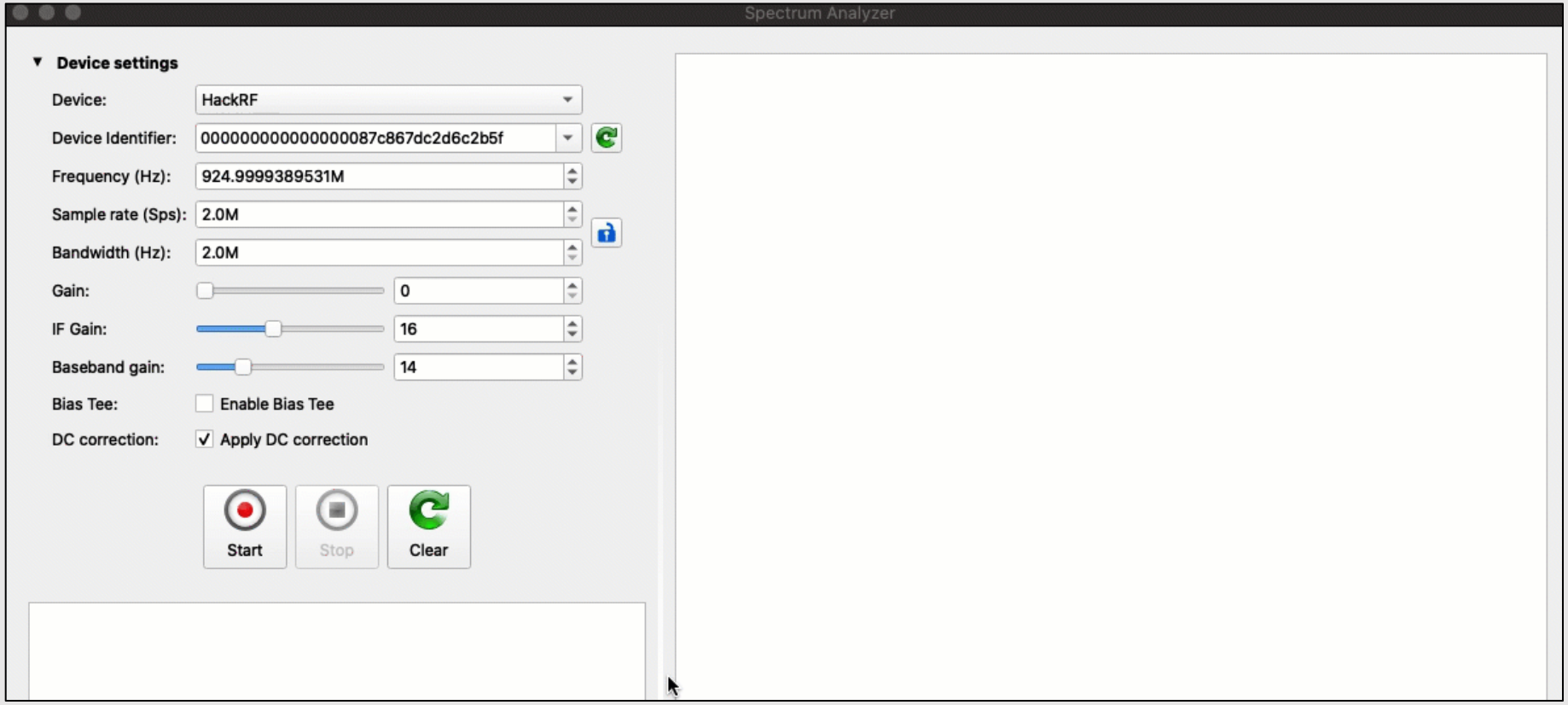
Recon: Equipment

- https://github.com/jopohl/urh
  - `pipenv install ipython, cython, urh, rfcat, pyserial, pyusb, pymodbus, cryptography`

- https://greatscottgadgets.com/hackrf/one

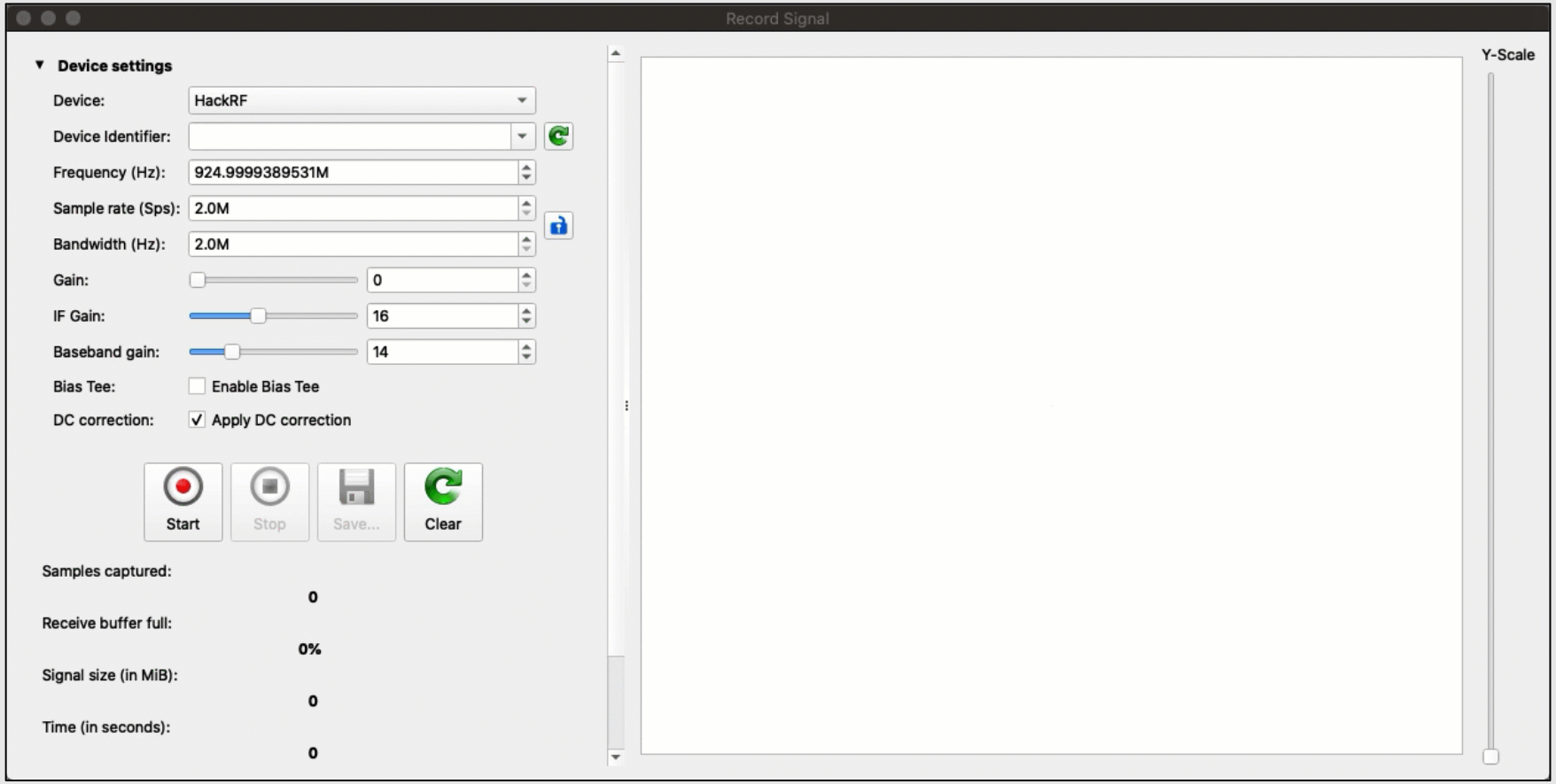
Capture: Locate Transmissions

- Open Spectrum Analyzer Window
- Select your radio and configure settings.
- Pick a frequency in the 900 MHz range.
- FHSS will hit frequencies over and over. Center on one.



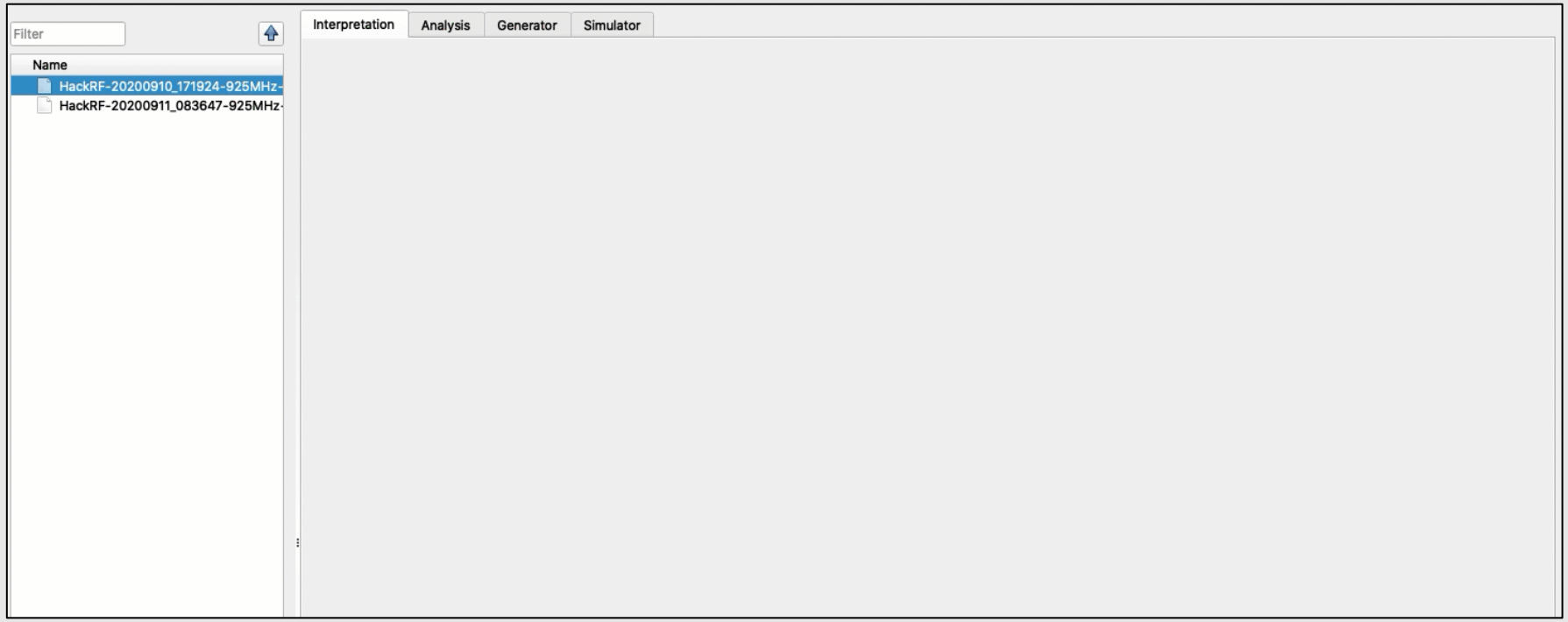
Capture: Record Transmissions

- Open Record Signal Window.
- Select radio and double check settings.
- Record Transmissions watching file size.
- Save capture with filename that documents capture settings.



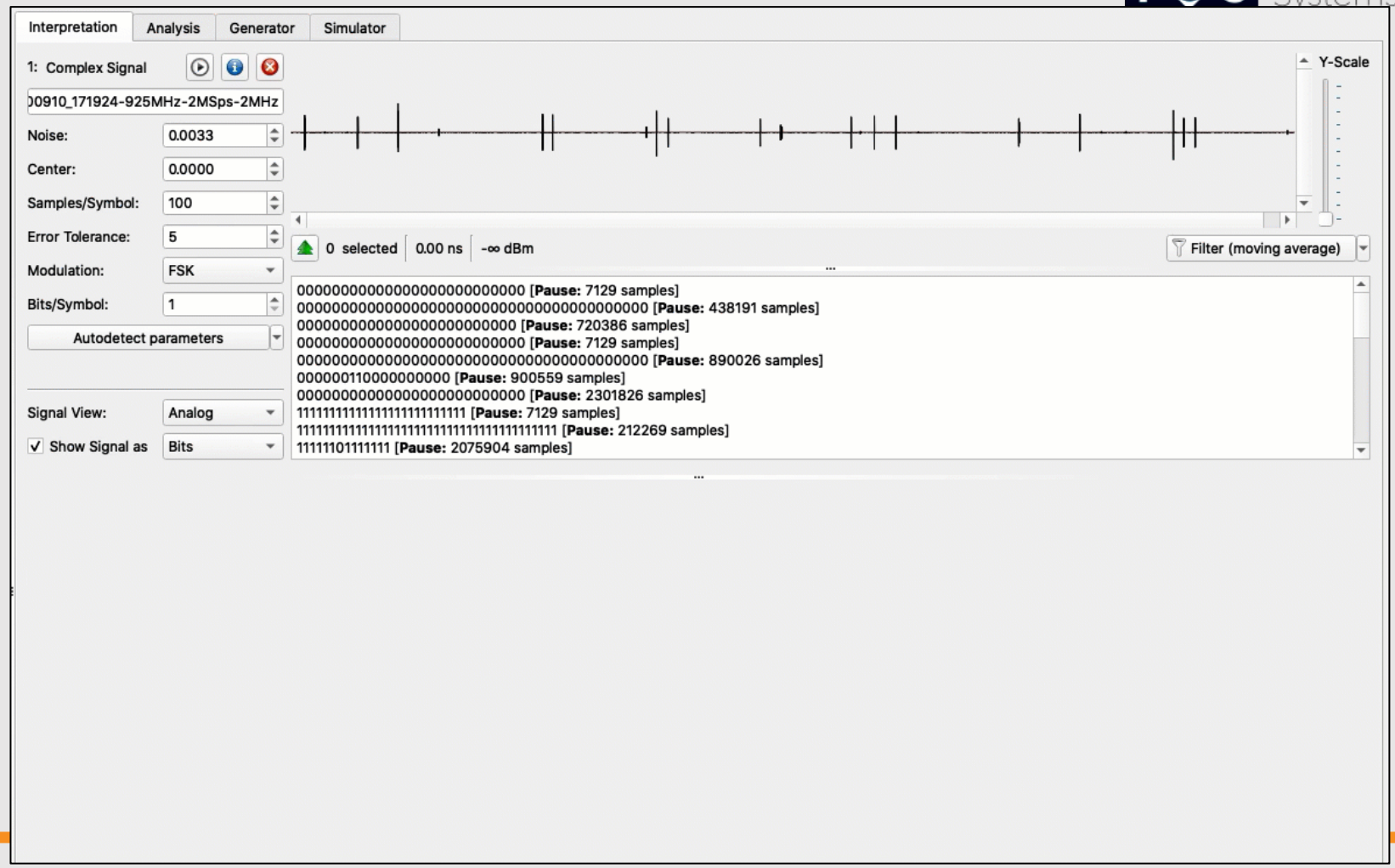
Analysis: Adjust Noise

- Drag capture file into "Interpretation" window.
- Review signal and adjust "noise" setting, if necessary.
- Setting "noise" too high will obfuscate some transmissions.
- Hackrf reduces noise well, use URH autodetection.
- RTL-SDR users may have to adjust this setting.



Analysis: Isolate Transmission

- Select a transmission to analyze.
- Use the "Create signal from selection" option.
- Crop new signal to help with review and file size.
- Change "Signal View" from "Analog" to "Demodulated".
- Locate demodulated signal and review for a good transmission type and signal capture.

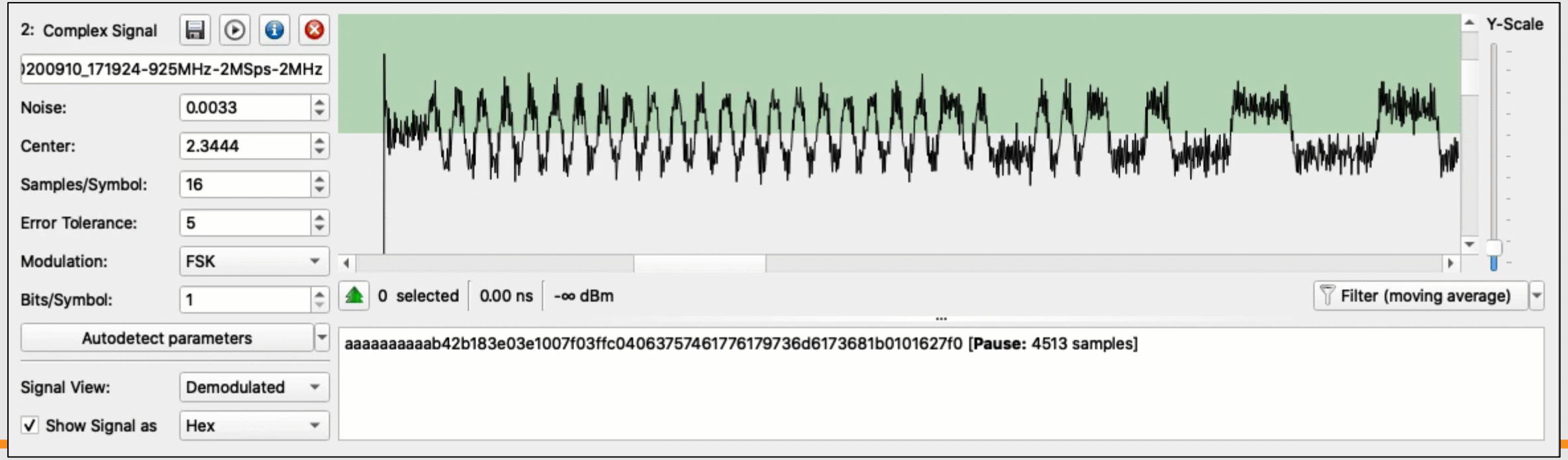


Analysis: Adjust Processing Parameters

- Adjust "Center" because this data was not transmitted on center frequency.
- Use signal spikes to adjust center line equally between spikes and troughs.
- Locate the part of the transmission with the shortest wave transition across the center line.
- Highlight a single wave and note the time. Spikes and troughs should cross center line in equal amount of time.
- Time for a single spike (or trough) is the value to use for Samples / Symbol setting.
- Set "Show Signal as" to "Hex" and review for demodulated data for potential preamble and sync word.
- If you expect a string, change "Show Signal as" to "ASCII" and review demodulated data for string.

Analysis: Preamble / Sync Word Review

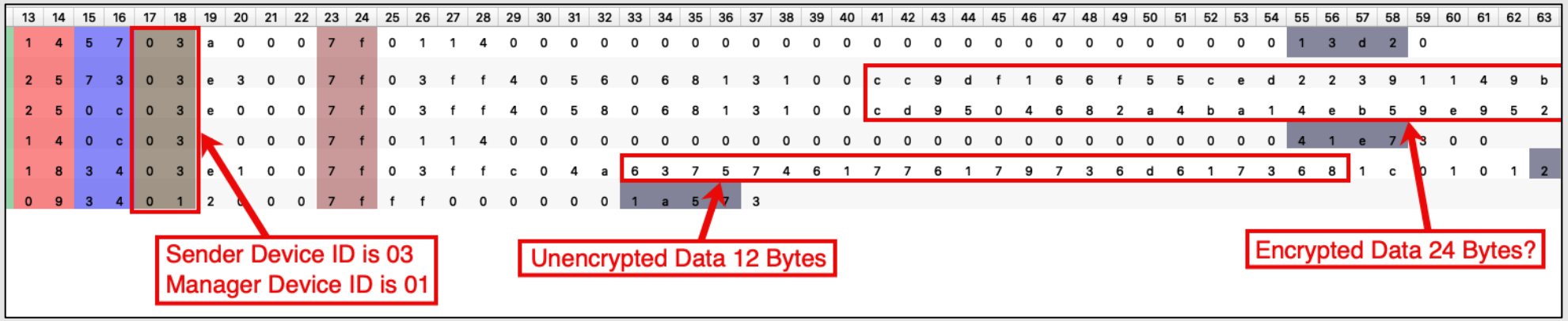
- Data from signal will not always be obvious and require review / adjustment.
- Adjust the "Show Signal as" setting between "Bits" and "Hex".
- Review display for known values.
- Crop signal to ensure signal starts with "1" bit.
- Crop signal to bit shift values to identify bit shifted sync word.
- Crop excessive preamble bits / bytes.



Analysis: Packet Field Identification

- Use "Analysis" tab to review packet contents.
- Highlight packet contents and label "nibble" groups according to their purpose. Add '?' if guessing.
- Configure "checksum" label to calculate CRC.
- Adjust "checksum" byte order to match packet data.

Analysis: Encrypted Packet Identification



Interesting Encryption Facts

> Wireless communication is based on Trusted Wireless 2.0 technology. The high demand for a interference-free data transmission using the license-free 900 MHz band, in particular via the use of the FHSS method (FHSS) and 128-bit data encryption (AES), is fulfilled.

- RAD-900-IFS datasheet indicates 128-bit data encryption (AES).
- Silicon Labs Si4463 Radio and Si4112 RF Synthesizer datasheets do not describe on-chip encryption or the implementation of AES.
- Texas Instruments MSP430F5438A datasheet does not describe on-chip encryption or the implementation of AES.

- So many questions:
  - AES uses 16-byte block size and IV should equal block size
    - "cutawaysmash" = 12 bytes
    - Encrypted data = 24 bytes? 16 bytes of data + 8 bytes of IV?
  - Management packets are not encrypted
  - Only data is encrypted, not full packet

Assessment Continued…

- Encryption Analysis
  - Send data with different byte lengths playing with block boundaries.
  - Send same data using different keys and key lengths.
  - Phoenix Contact PSI Conf accepts key lengths of "min. 4, max 16 characters".
- Retransmit packets
  - Properly configure URH to resend captured packets via HackRF
  - Configure Yardstick One to send packet using rfcat
- Determine if radio protocol can be used for Denial-of-Service attacks.
- Redo all testing using Modbus commands to control end-points.

Conclusion

- Understand your process and ensure it can operate when the radios cannot communicate.
- Default settings are not encrypted and can be intercepted and analyzed.
- Test to verify requirements after implementation and maintenance.
- Support research into toolsets that help conduct assessments to ensure proper implementation.

References

- https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2901540&library=usen&tab=2
- https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=1931025
- https://www.silabs.com/documents/public/data-sheets/Si4464-63-61-60.pdf
- https://www.silabs.com/documents/public/data-sheets/si4133.pdf
- https://www.silabs.com/documents/public/application-notes/AN626.pdf
- https://www.ti.com/lit/ds/symlink/msp430f5438a.pdf?ts=1599849269002&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FMSP430F5438A
- https://www.willhackforsushi.com/presentations/Essential_Crypto_Without_the_Math_Webcast-20100426.pdf

CUTAWAY SECURITY
INFOSEC CONSULTANTS

Don C. Weber - @cutaway
don@cutawaysecurity.com
https://www.cutawaysecurity.com

Thomas Van Norman
https://www.icsvillage.com/contact-us