

Industrial
Control
Systems



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —



Detecting Encrypted Radio Communications Using Universal Radio Hacker

Don C. Weber - @cutaway

Principal Consultant, Founder

© 2020 Cutaway Security, LLC. All Rights Reserved.

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



Cutaway Security, LLC / Don C. Weber



- ICS Security Assessments
- Penetration Testing
- Security Research



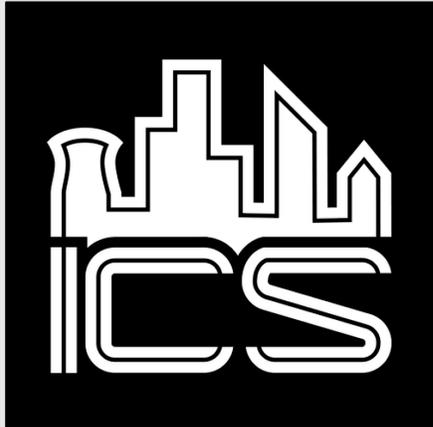
SANS ICS410: ICS/SCADA Security Essentials



Assessing and Exploiting Control Systems



Special Thanks



ICS410 ICS/SCADA Security Essentials

A mix of hands-on and theoretical class, being driven by a high skilled instructor, makes this the best training in ICS security.

Rafael Issa, Technip

About the course

ICS410 is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.



ICS410 Challenge Coin

REGISTER TODAY



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



**Analyzing Radio
Transmissions Using URH**

<https://www.cutawaysecurity.com>



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



Why are we here?



Point-to-point connections

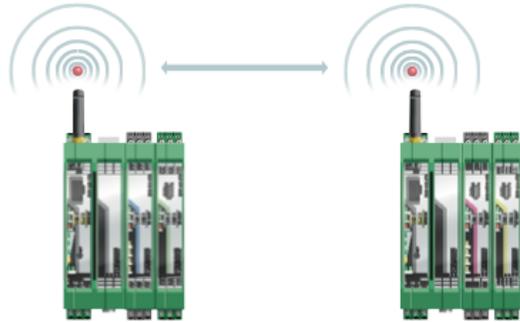
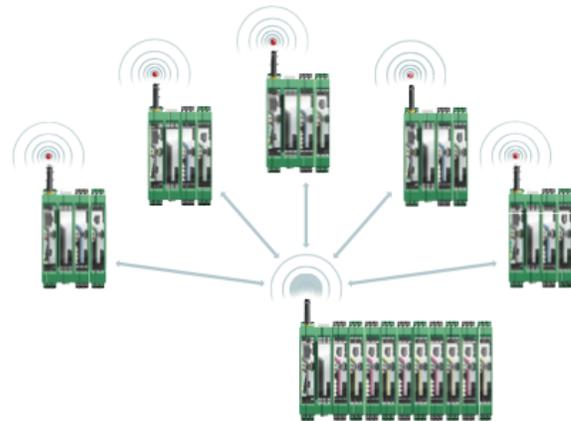


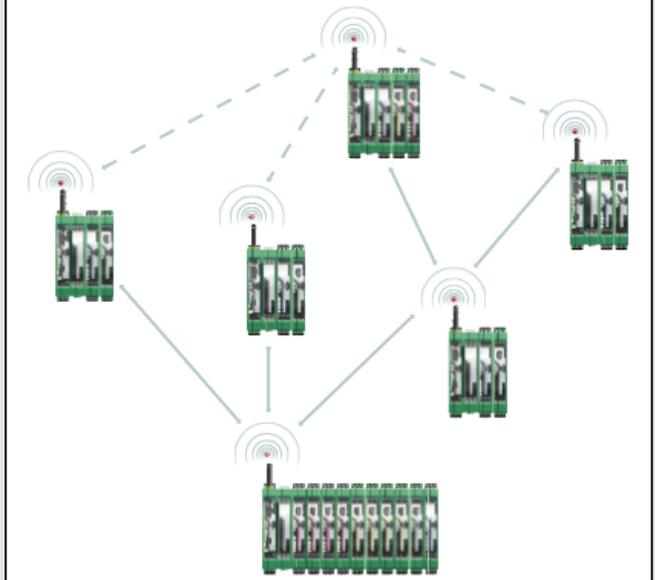
Figure 12 Example of point-to-point connection

Star network



- 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.

Self-healing network



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

Encryption Off by Default

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

```
Windows PowerShell
PS CutSec 09/09/2020 14:05:38
> Select-String *.*.dat -Pattern Encryption
radio_preso_serial-rad-900_20200907.dat:18:RadioEncryptionEnabled=False
radio_preso_serial-rad-900_20200907.dat:19:RadioEncryptionKey=
radio_preso_serial_enc-rad-900_20200909.dat:18:RadioEncryptionEnabled=True
radio_preso_serial_enc-rad-900_20200909.dat:19:RadioEncryptionKey=0000
PS CutSec 09/09/2020 14:05:40
```

Confidential Encryption Detection Technique

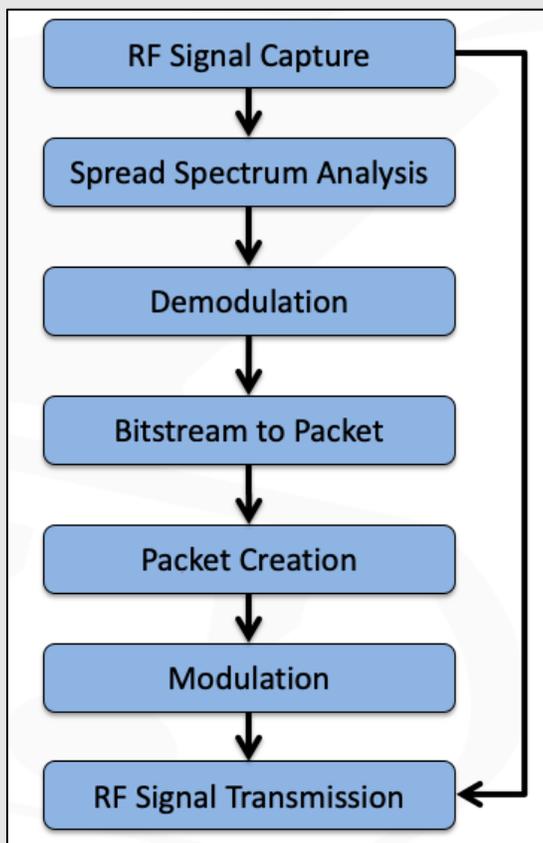
Configuration Without Encryption

Configuration With Encryption

- * Phoenix Contact RAD-900-IFS, in this example
- ** You'll be on Windows, so `Select-String *.*.dat -Pattern Encryption`
- *** Mitigate here, if these are your radios. If not, note "Key" value.
- **** ???? is shorthand for Report / Document



Active Wireless Radio Assessment Methodology



- 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...

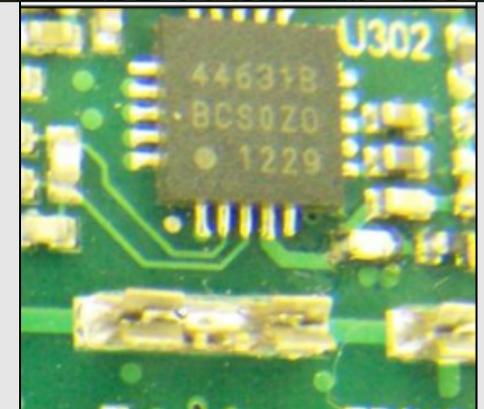
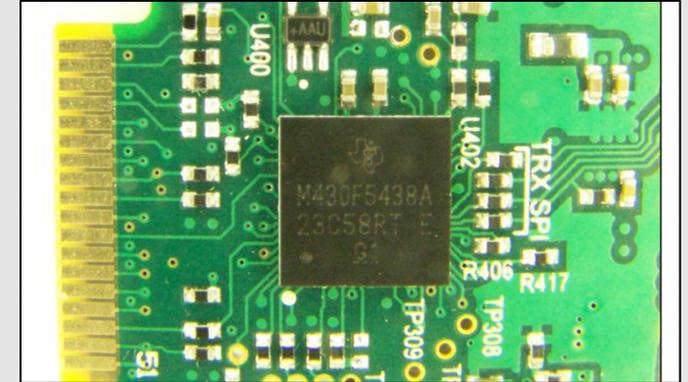
Source: ControlThings.io Accessing and Exploiting Control Systems
<https://www.controlthings.io/training>



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: $X^{15}+X^{12}+X^5+1$ 16-bit polynomial
 - Example code from SI Packet Handler Operation For Si446x RFICs datasheet



Source: RAD-900 FCC Documentation



Recon: Equipment



Universal Radio Hacker
Investigate Wireless Protocols Like A Boss

- <https://github.com/jopohl/urh>
 - ``pipenv install ipython, cython, urh, rfc4, pyserial, pyusb, pymodbus, cryptography``



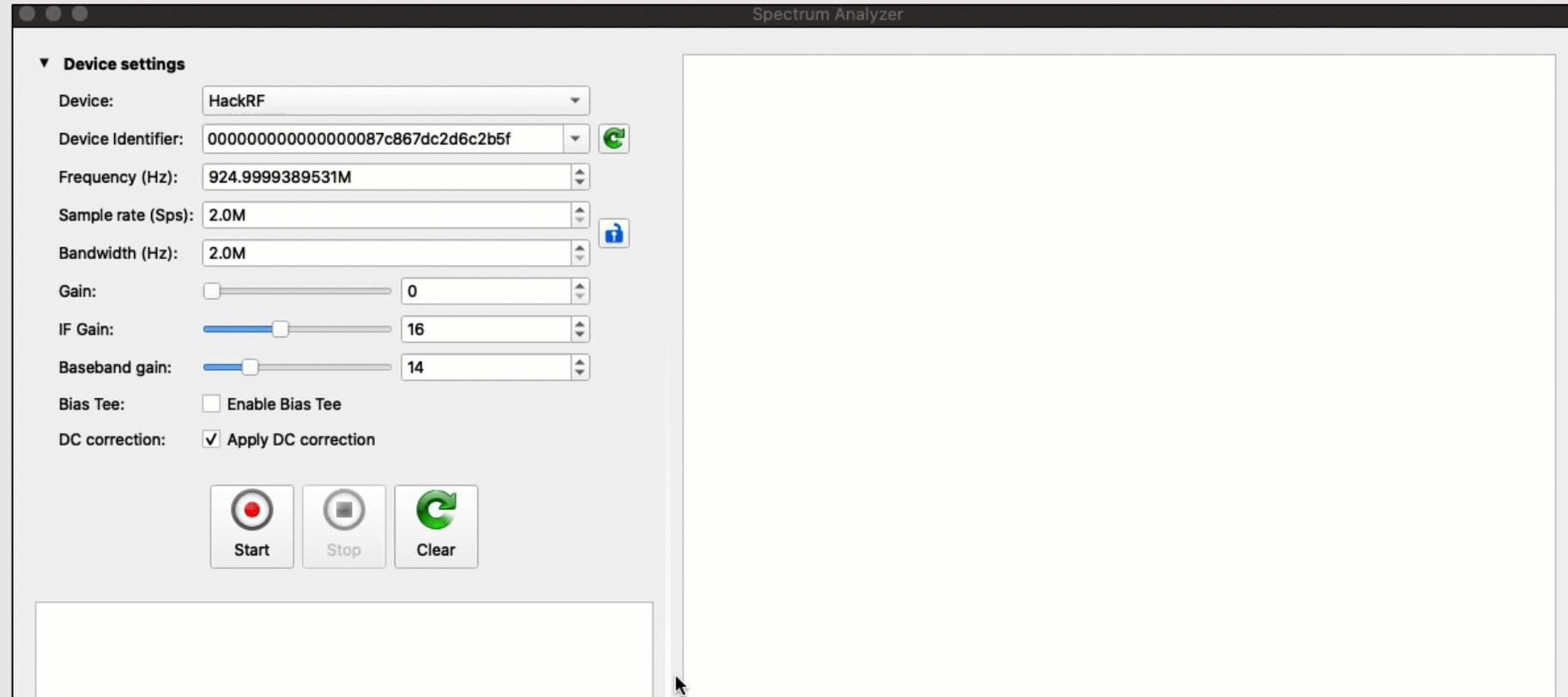
- <https://greatscottgadgets.com/hackrf/one>



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.

Record Signal

▼ Device settings

Device: HackRF

Device Identifier: []

Frequency (Hz): 924.9999389531M

Sample rate (Sps): 2.0M

Bandwidth (Hz): 2.0M

Gain: [] 0

IF Gain: [] 16

Baseband gain: [] 14

Bias Tee: Enable Bias Tee

DC correction: Apply DC correction

Start Stop Save... Clear

Samples captured: 0

Receive buffer full: 0%

Signal size (in MiB): 0

Time (in seconds): 0

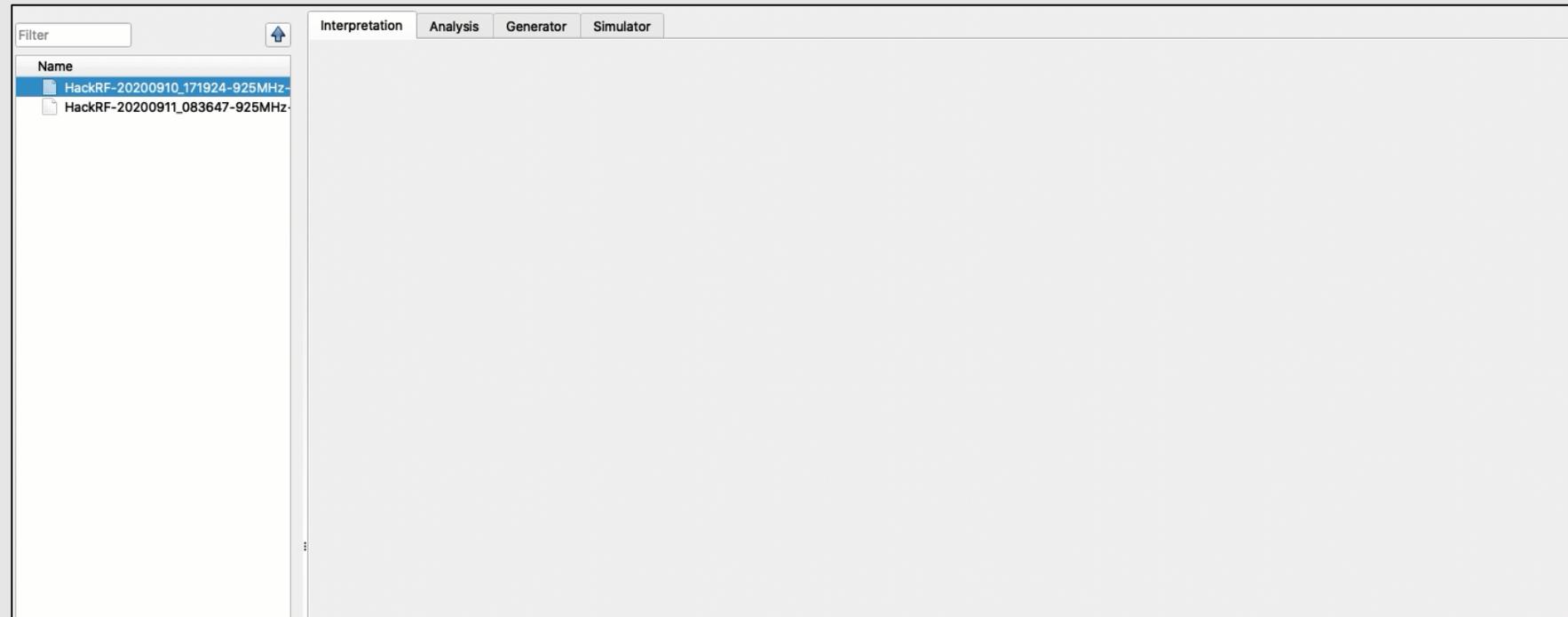
Y-Scale



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.

The screenshot displays a software interface for signal analysis. The top menu bar includes "Interpretation", "Analysis", "Generator", and "Simulator". The main window shows a signal analysis for a "Complex Signal" with the following parameters:

- Signal: 00910_171924-925MHz-2MSps-2MHz
- Noise: 0.0033
- Center: 0.0000
- Samples/Symbol: 100
- Error Tolerance: 5
- Modulation: FSK
- Bits/Symbol: 1

The "Signal View" is set to "Analog", and "Show Signal as" is set to "Bits". The waveform shows a series of pulses. Below the waveform, the demodulated bitstream is displayed, showing a sequence of 0s and 1s with pause times in samples:

```
00000000000000000000000000000000 [Pause: 7129 samples]
0000000000000000000000000000000000000000000000000000000 [Pause: 438191 samples]
00000000000000000000000000000000000000000000000000 [Pause: 720386 samples]
000000000000000000000000000000000000000000000000000 [Pause: 7129 samples]
0000000000000000000000000000000000000000000000000000 [Pause: 890026 samples]
00000011000000000000 [Pause: 900559 samples]
00000000000000000000000000000000000000000000000000 [Pause: 2301826 samples]
1111111111111111111111111111111111 [Pause: 7129 samples]
1111111111111111111111111111111111111111111111111111 [Pause: 212269 samples]
1111101111111 [Pause: 2075904 samples]
```




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.

The screenshot displays a signal analysis interface. On the left, a control panel shows the following settings: "2: Complex Signal", "200910_171924-925MHz-2MSps-2MHz", Noise: 0.0033, Center: 2.3444, Samples/Symbol: 16, Error Tolerance: 5, Modulation: FSK, Bits/Symbol: 1, and "Autodetect parameters". The "Signal View" is set to "Demodulated" and "Show Signal as" is set to "Hex". The main display area shows a waveform of a demodulated signal. Below the waveform, the hexadecimal data is shown as: `aaaaaaaaab42b183e03e1007f03ffc04063757461776179736d6173681b0101627f0 [Pause: 4513 samples]`. A "Filter (moving average)" dropdown is visible in the bottom right corner of the waveform area.



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.

The screenshot displays the 'Analysis' tab of the SANS ICS software. The interface is divided into several sections:

- Protocols/Participants:** A tree view on the left shows a 'New Group' containing two items: 'HackRF-20200910_171924-925MHz...' and 'rad-900_pkt0_HackRF-20200910...'. The second item is selected.
- View data as:** Set to 'Hex'.
- Decoding:** Set to 'Non Return To Zero (NRZ)'. Decoding errors are 0 (0.00%).
- Options:** Three checkboxes are present: 'Mark diffs in protocol', 'Show only diffs in protocol', and 'Show only labels in protocol', all of which are unchecked.
- Analyze Protocol:** A dropdown menu is set to 'Analyze Protocol'.
- Search:** A search bar with the text 'Enter pattern here' and a search icon.
- Packet Data:** A table showing the packet's bit stream. The first row contains 41 columns, each representing a bit. The bits are: 1, a, a, a, a, a, a, a, a, b, 4, 2, b, 1, 8, 3, e, 0, 3, e, 1, 0, 0, 7, f, 0, 3, f, f, c, 0, 4, 0, 6, 3, 7, 5, 7, 4, 6, 1, 7.
- Message types:** A table with columns for Name, Color, Display format, Order [Bit/Byte], and Value. The 'Default' message type is checked.
- Bottom Status:** Shows 'Bit: 00000011', 'Hex: 03', 'Decimal: 3', and '2 column(s) selected'.



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 rfcatt
- 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



Industrial
Control
Systems



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —



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

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



ICS410 ICS/SCADA
Security Essentials

A mix of hands-on and theoretical class, being driven by a high skilled instructor, makes this the best training in ICS security.

Rafael Issa, Technip

About the course

ICS410 is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

REGISTER TODAY



ICS410 Challenge Coin