September 17, 2024

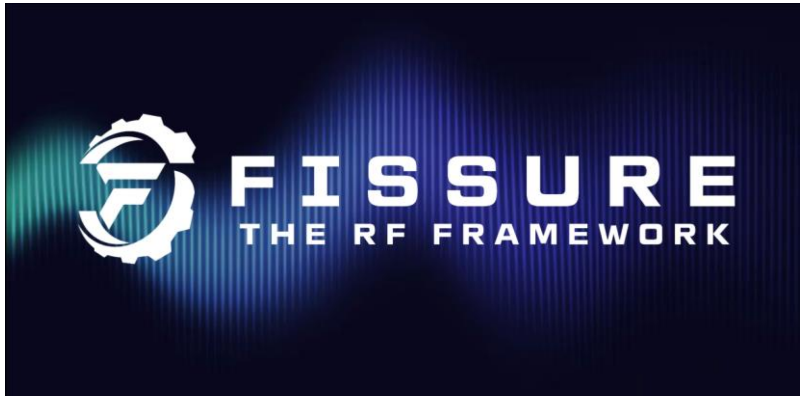
Remote Sensor Node Updates for FISSURE – The RF Framework

GNU Radio Conference 2024

Christopher Poore
Senior Reverse Engineer
Assured Information Security, Inc.
poorec@ainfosec.com

Agenda

- FISSURE Overview
- Why FISSURE
- Remote Sensor Node Updates
- Demonstration
  - Sensor Node Configuration
  - Transmit/Receive Capabilities
  - Autorun Playlists
  - Triggers



Components

- Target Signal Identification
- Protocol Discovery
- Attacks
- IQ Manipulation
- Online Signal Archive
- Packet Crafting
- Third-Party Tools
- Lessons

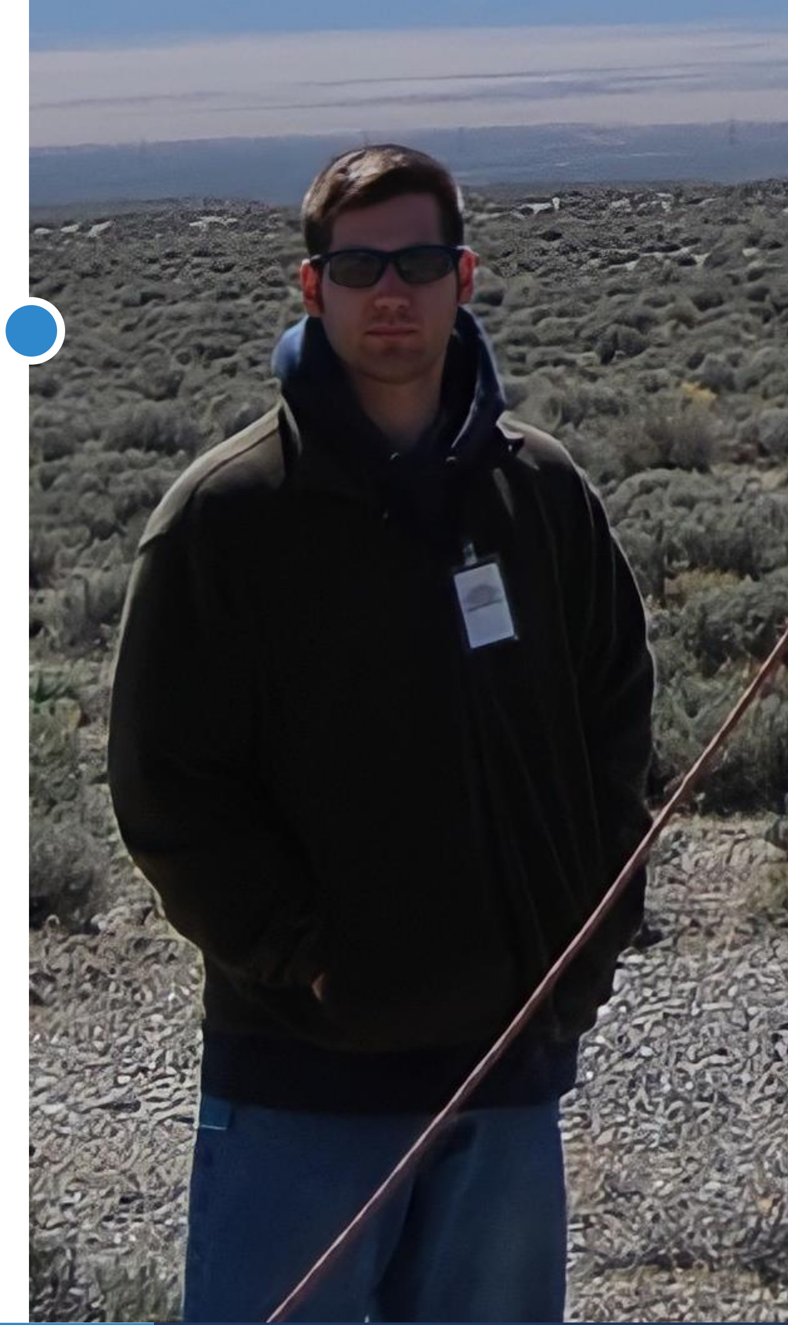
8 September 27, 2022 FISSURE: The RF Framework – github.com/ainfosec/FISSURE Chris Poore - poorec@ainfosec.com ASSURED INFORMATION SECURITY

Introduction

Mr. Chris Poore
AIS, *Senior Reverse Engineer*

Expertise

- Part of a team that does security testing, functional testing, research, penetration testing, offensive/defensive cyber operations
- Discovering vulnerabilities in wireless systems
- Gaining access to systems via RF
- Reverse engineering RF protocols
- Forensically testing cybersecurity systems
- Administering RF collection events
- Developing open-source software for RF applications
- Researching cutting-edge solutions in RF and cyber



Assured Information Security

About AIS

- Cyber and Information Security
  - Research
  - Development
  - Consulting
  - Testing
  - Forensics
  - Remediation and Training
- Headquartered in Rome, New York
- Government and Commercial Customers
- 200+ employees

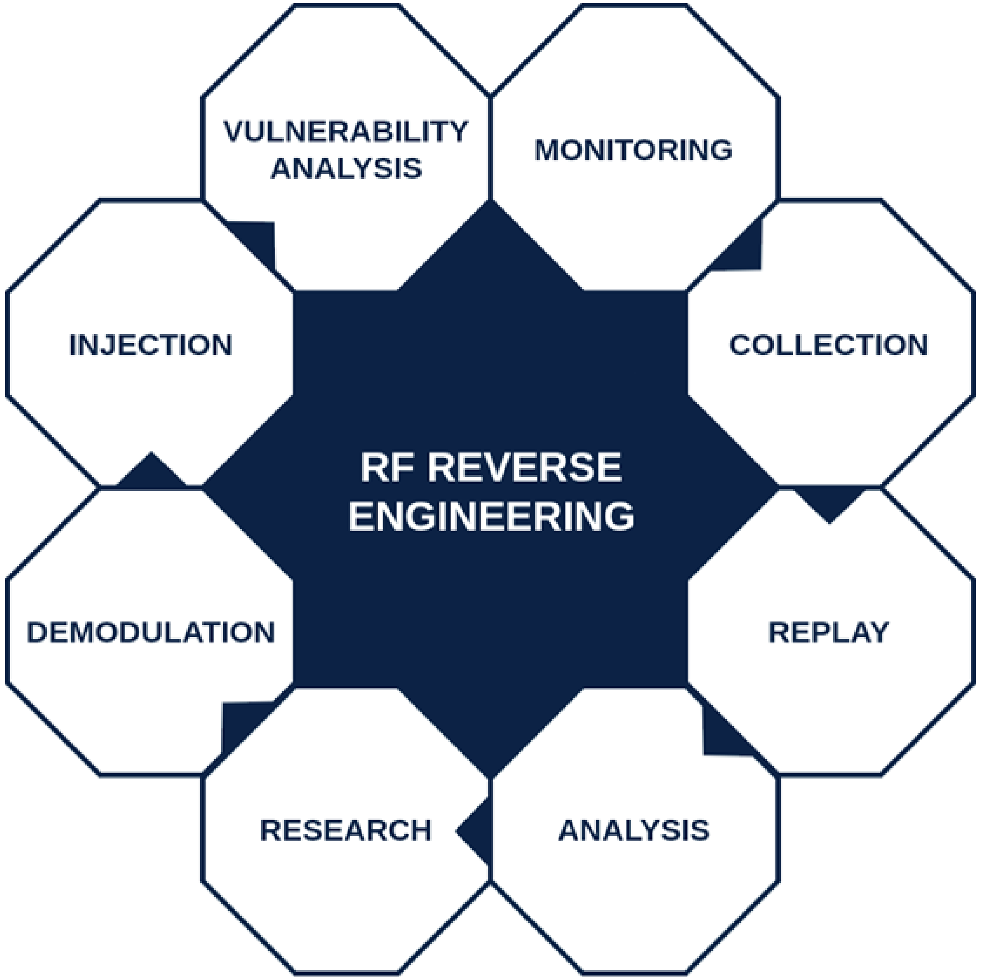
- Core Capabilities:
  - Advanced Research
  - Cyber Operations
  - Intelligence Analysis
  - Security Testing
  - Trusted Systems

ainfosec.com

FISSURE – The RF Framework

Summary

- Open-source RF and reverse engineering framework on GitHub since August 2022
- Contains hooks for detection, classification, protocol discovery, attack execution, vulnerability analysis, automation, AI/ML
- Consolidates all-things RF: software modules, radios, protocols, signal data, scripts, flow graphs, reference material, and third-party tools
- Speeds up the characterization of signals and the identification of vulnerabilities in RF protocols, waveforms, and devices
- Mostly Python & PyQt with support for legacy systems
- Out-of-the-box, transparent, pain-free software installer
- Meant for everyone: experts and beginners, easily edit pieces on your own
- We seek to increase contributors, promote collaboration, and foster education



Why FISSURE?

- **Stage** your computer with hundreds of tools, avoid starting from scratch
- **Reuse** your code to eliminate waste
- **Learn** about new technologies, signals, and programming
- **Discover** areas for improvement within FISSURE, contribute your ideas
- **Build** something, advertise it, get famous, find meaning
- **Share** success, network with others, grow professionally

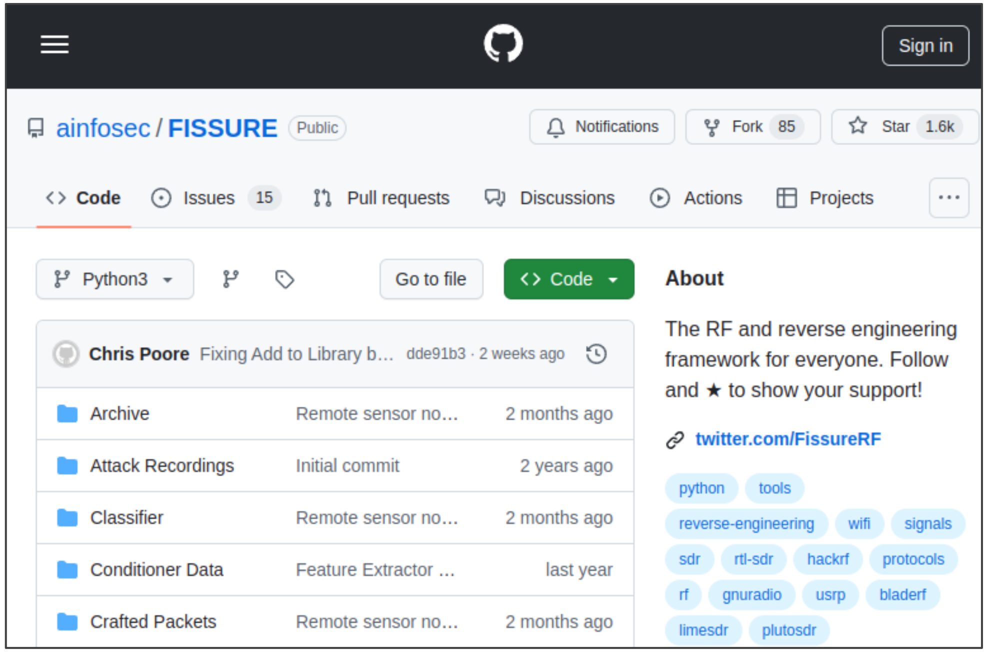
FISSURE
THE RF FRAMEWORK

GNU Radio Aspects

Points of Interest

- Install multiple out-of-tree modules at once with a single click
- Quickly access/store flow graphs with the FISSURE menu and library
- Launch flow graphs for live inspection or on signal recordings
- Download collections of signals from an online archive for testing and development
- View default variables for flow graphs in tables and change values during runtime
- Build playlists and apply triggers for flow graphs
- Offers backwards compatibility for multiple GNU Radio versions

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM



ainfosec / FISSURE Public

Chris Poore Fixing Add to Library b… dde91b3 · 2 weeks ago

Archive	Remote sensor no…	2 months ago
Attack Recordings	Initial commit	2 years ago
Classifier	Remote sensor no…	2 months ago
Conditioner Data	Feature Extractor …	last year
Crafted Packets	Remote sensor no…	2 months ago

About

The RF and reverse engineering framework for everyone. Follow and ★ to show your support!

twitter.com/FissureRF

python tools reverse-engineering wifi signals sdr rtl-sdr hackrf protocols rf gnuradio usrp bladerf limesdr plutosdr

Operational Flow

Intended Sequence of Actions

- Provide visualizations, tools, algorithms, AI/ML techniques for supporting each phase in the RF Reverse Engineering process
- **Target Signal Identification Tab**
  - Obtain signals of interest with some preliminary analysis
- **Protocol Discovery Tab**
  - Identify RF protocol parameters for demodulation and perform analysis of the bitstream, expand FISSURE library with protocol information
- **Attack Tab**
  - Execute single-stage, multi-stage, or fuzzing attacks using third-party tools, Python scripts, GNU Radio flow graphs, and crafted packets from the FISSURE library
- **IQ Data Tab**
  - Perform manual analysis of signal data through recording, playback, live inspection, data manipulation, filtering, and viewing

Operational Flow

Intended Sequence of Actions

- **Archive Tab**
  - Download signal file collections from the AIS online archive, build signal playlists, construct datasets with randomizations for machine learning training
- **Sensor Nodes Tab**
  - Construct autorun playlists from single-stage and multi-stage attacks to run on remote sensor nodes, perform file transfer functions between the remote sensor nodes and the local workstation
- **Library Tab**
  - Browse/search the FISSURE library, view saved user images, add/remove: protocols, modulation types, packet types, signals of interest, statistics, demodulation flow graphs, attacks
- **Log Tab**
  - View and filter the system log, set logging levels, create session notes
- **Menu Items**
  - Browse options, customize color schemes, open standalone flow graphs, experiment with third-party tools, view reference material and lessons, access help items and local user manual

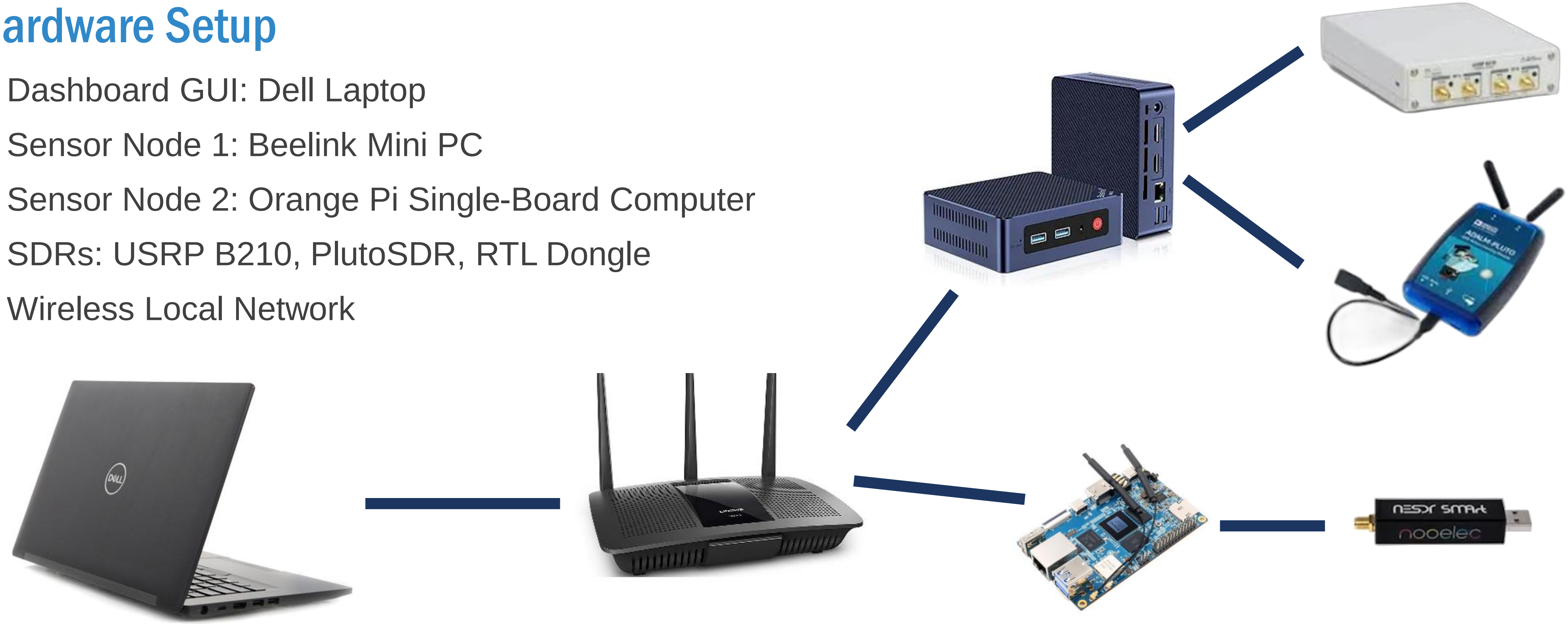
Remote Sensor Node Updates

- Remote computing nodes that support many types of radio peripherals
- Runs scripted playlists on startup or through user interaction
- Saves data local to the sensor node and can transfer it over a network
- Maintains existing FISSURE capabilities
- Can communicate on a standalone FISSURE instance, across a local network, or over the internet

Sensor Node Example

Hardware Setup

- Dashboard GUI: Dell Laptop
- Sensor Node 1: Beelink Mini PC
- Sensor Node 2: Orange Pi Single-Board Computer
- SDRs: USRP B210, PlutoSDR, RTL Dongle
- Wireless Local Network



Sensor Node Benefits

- Low-cost, versatile hardware options
- Flexible software solution that supports integration
- Open-source nature provides unique levels of access
- Education and training tool
- Provides remote workers a mechanism for RF testing
- Widens access to specialized RF environments: international localities, laboratories, test sites

- Unlocks many geospatial scenarios for FISSURE
    - Direction Finding
    - Tracking
    - Intrusion Detection
    - Mobile Deployment
    - Perimeter Defense

OPEN ARCHITECTURE RESILIENT IOT FOR OPERATIONAL NETWORKS

ORION

orionassured.com

ORION is a technology accelerator and innovation ecosystem aimed at augmenting the US Air Force's ability to develop, secure, deploy and utilize devices comprising the Internet of Things (IoT) and the Internet of Military Things (IoMT).

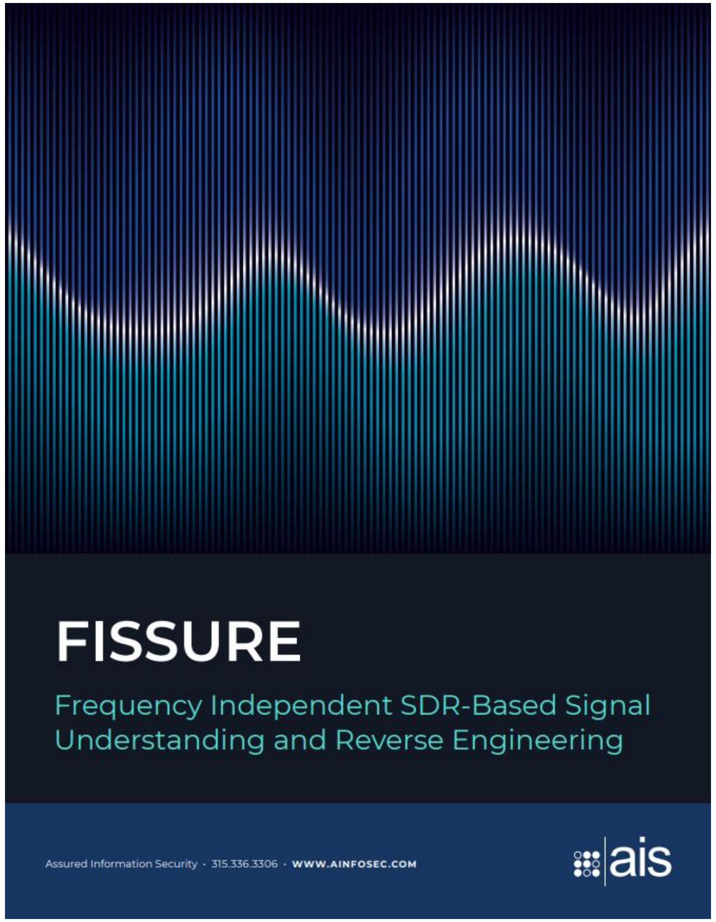
AIS Role in ORION:

- Provide cyber embedded systems SME
- Provide T&E models, capabilities, and personnel
- Provide bespoke testing facilities and environments (NTROPEE)
- Provide technology transition SME
- Provide tooling that enhances test processes and automation
  - (e.g., HYRULE, FISSURE, AI/ML)

Demonstration

Project Outlook

- Complete the roadmap found on GitHub
- Produce more simulation capabilities and participate in RF simulation events
- Expand and coalesce the online archive of IQ files
- Test and improve the code through remote assessments
- Extend to academia, create classroom exercises
- Support new GNU Radio versions
- Produce more videos for YouTube and Twitter/X
- Experiment using remote nodes in different operational scenarios and more integrated platforms



FISSURE

Frequency Independent SDR-Based Signal Understanding and Reverse Engineering

Assured Information Security · 315.336.3306 · WWW.AINFOSEC.COM

ais

Learn More

- FISSURE
  - https://github.com/ainfosec/FISSURE
  - https://www.ainfosec.com/fissure
  - https://www.youtube.com/@assuredinformationsecurity
- AIS
  - https://www.ainfosec.com
- Twitter/X
  - @FissureRF

Chris Poore
Senior Reverse Engineer
poorec@ainfosec.com
Assured Information Security, Inc.

Questions

Chris Poore

Senior Reverse Engineer

poorec@ainfosec.com

Assured Information Security, Inc.