April 28, 2021

Eric Thayer

Chris Poore

FISSURE:

An RF Framework

Monthly Lecture
Education Series

+

GRIFFISS INSTITUTE

INNOVARE ADVANCEMENT CENTER

ais

Agenda

- Introduction
- RF Analysis
- Challenges
- Solution
- FISSURE capabilities
- Demonstration

Who are we?

Identify weaknesses

Evaluate design and implementation

Assess deployed software and hardware

Verify systems

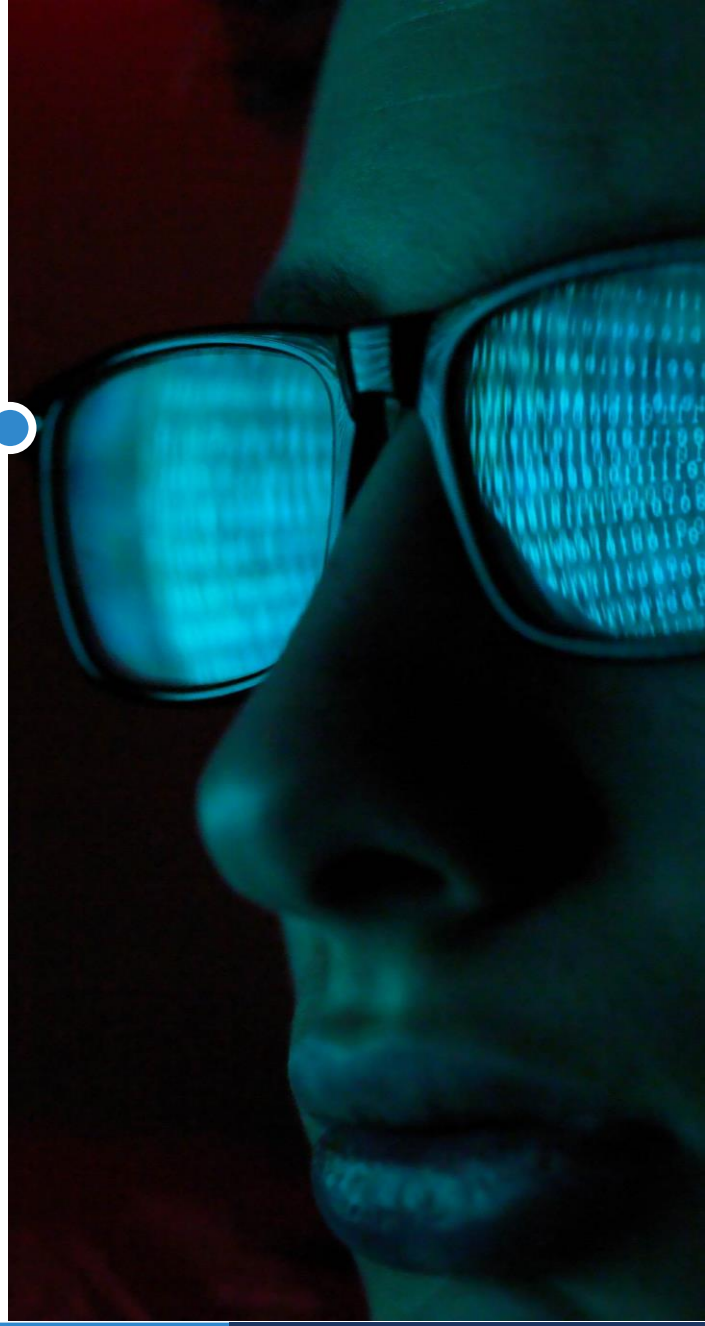
Make sure they are safe and secure

Detect issues before they are found by attackers

Provide solutions

Minimize risk through threat awareness

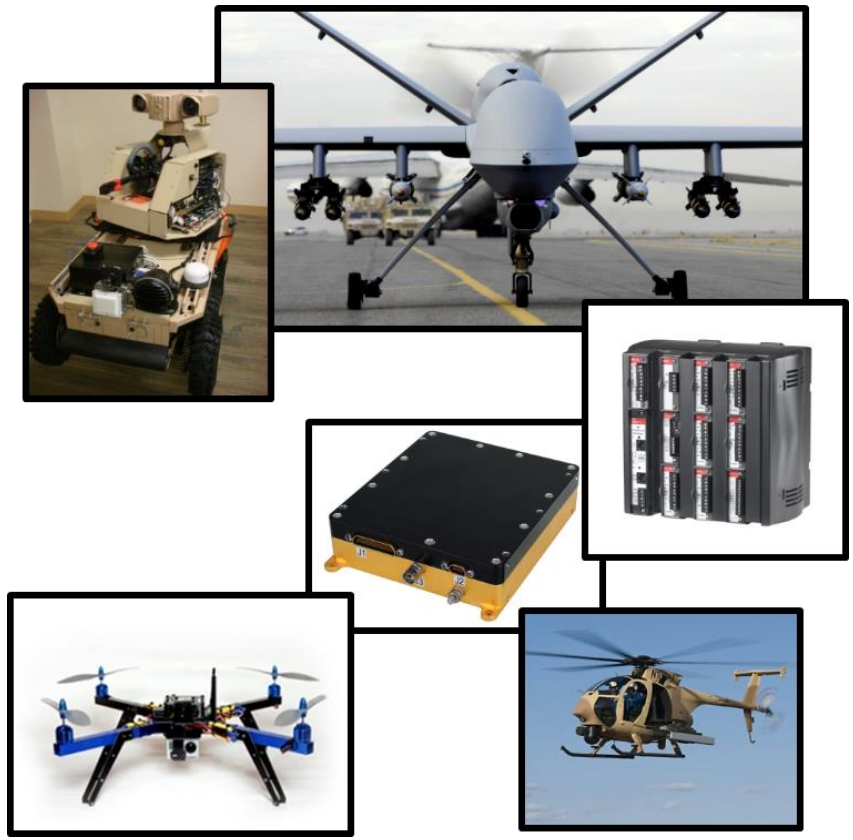
Develop techniques to mitigate threats



I. M. Hacker
AIS, *White Hat*

Why does RF matter?

- Cyber physical systems connect the digital world to the physical environment
  - Vehicles
  - Unmanned aerial systems
  - Communications networks
  - Industrial control systems
  - Medical devices
  - Weapon systems
- Radios are everywhere
  - Smart = connected
  - Connections expose attack vectors



Vulnerability Analysis Process

RF enabled systems

- Detect the presence of RF energy
- Understand the characteristics of the signal
- Collect and analyze samples
- Develop transmit and/or injection techniques
- Craft custom payloads or messages

The Process Has Challenges

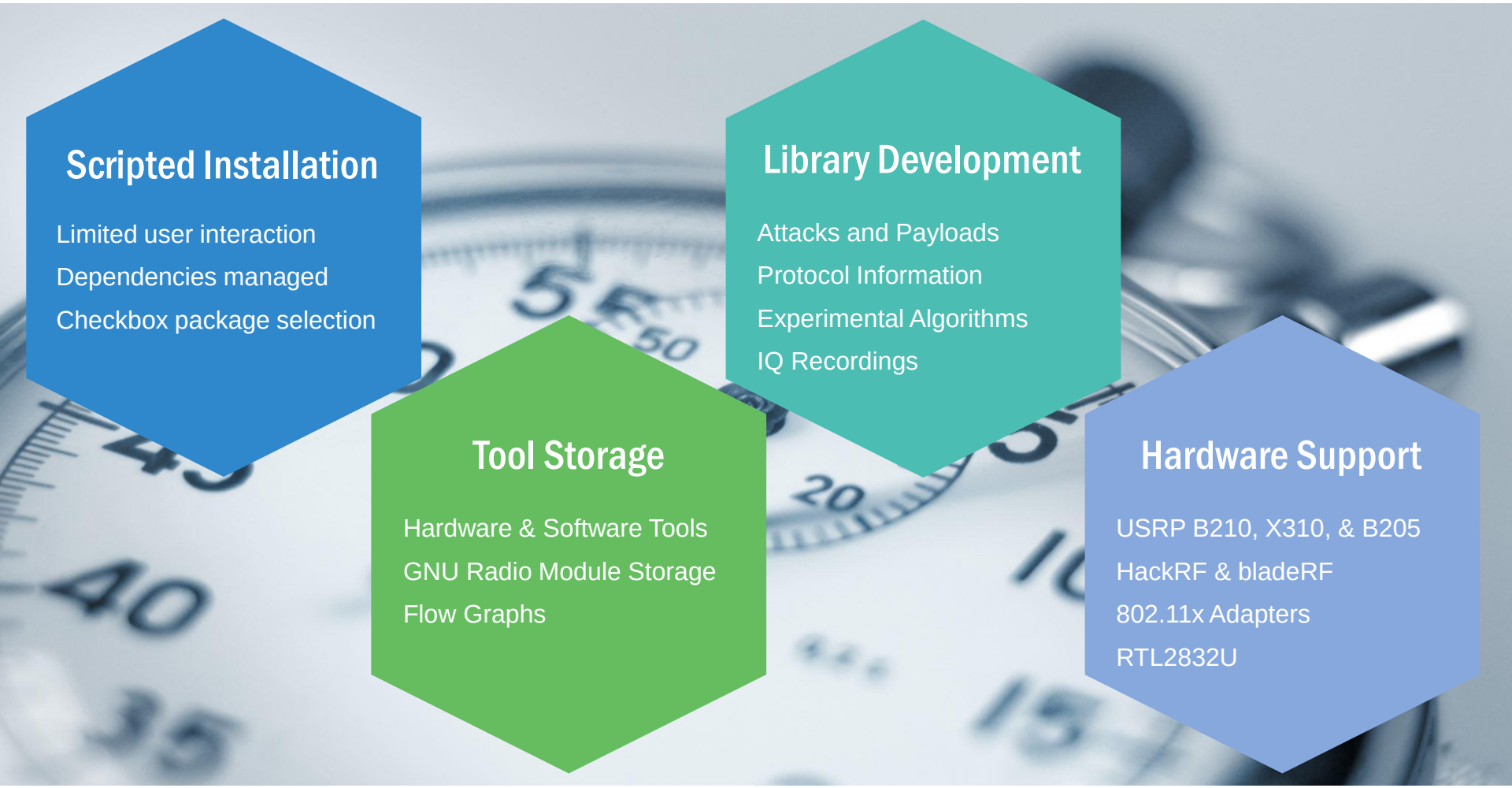
We have a solution!

- In-House laboratory tool designed to enable rapid detection, analysis, and transmission of RF signals
- Modular framework that simplifies development and integration of tools and hardware
- Repository of RF signals and attack tools

FISSURE

- An AIS developed tool to prototype techniques and perform RF device assessment
- A framework with hooks that enable
  - Detection
  - Classification
  - Protocol discovery
  - Attack execution
  - Vulnerability analysis
  - Automation
- A standardized interface for open source and one-off tools

Workflow Enabler



Scripted Installation

Limited user interaction
Dependencies managed
Checkbox package selection

Library Development

Attacks and Payloads
Protocol Information
Experimental Algorithms
IQ Recordings

Tool Storage

Hardware & Software Tools
GNU Radio Module Storage
Flow Graphs

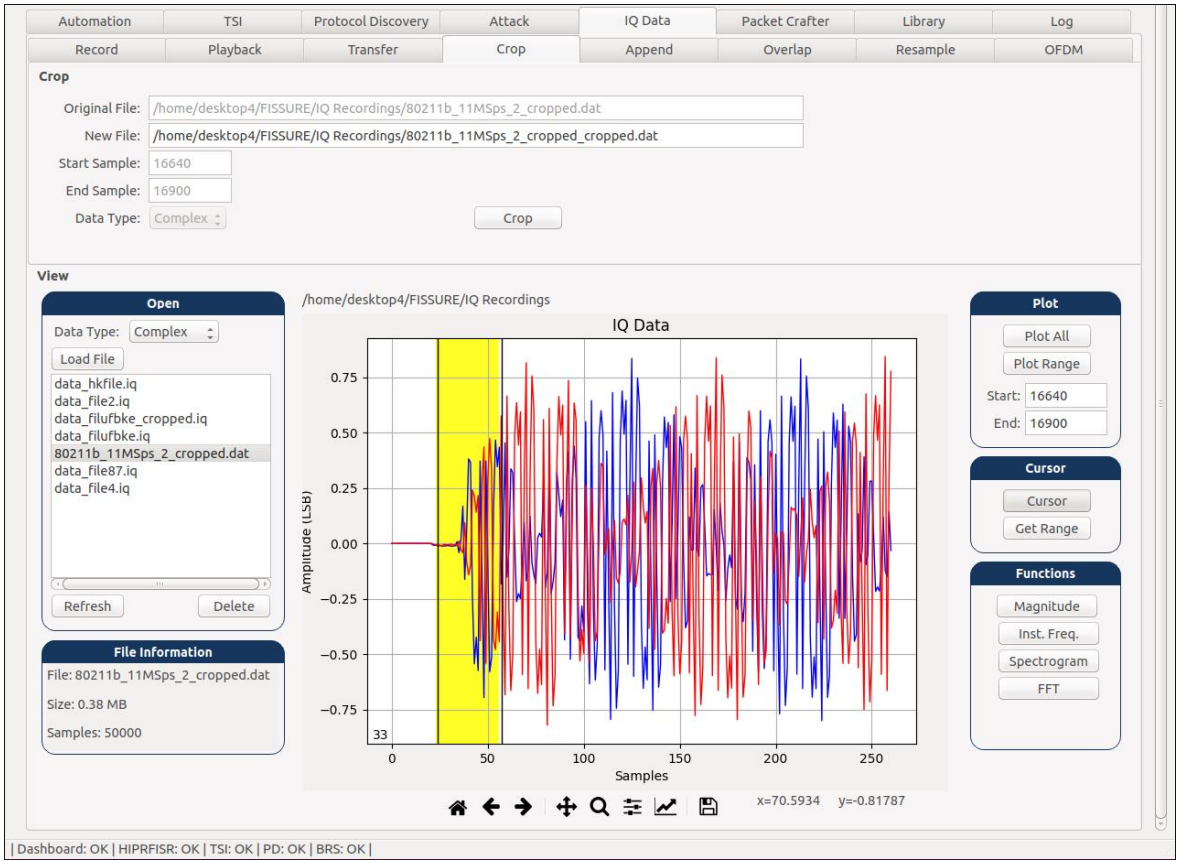
Hardware Support

USRP B210, X310, & B205
HackRF & bladeRF
802.11x Adapters
RTL2832U

Current Features

Work with raw IQ data

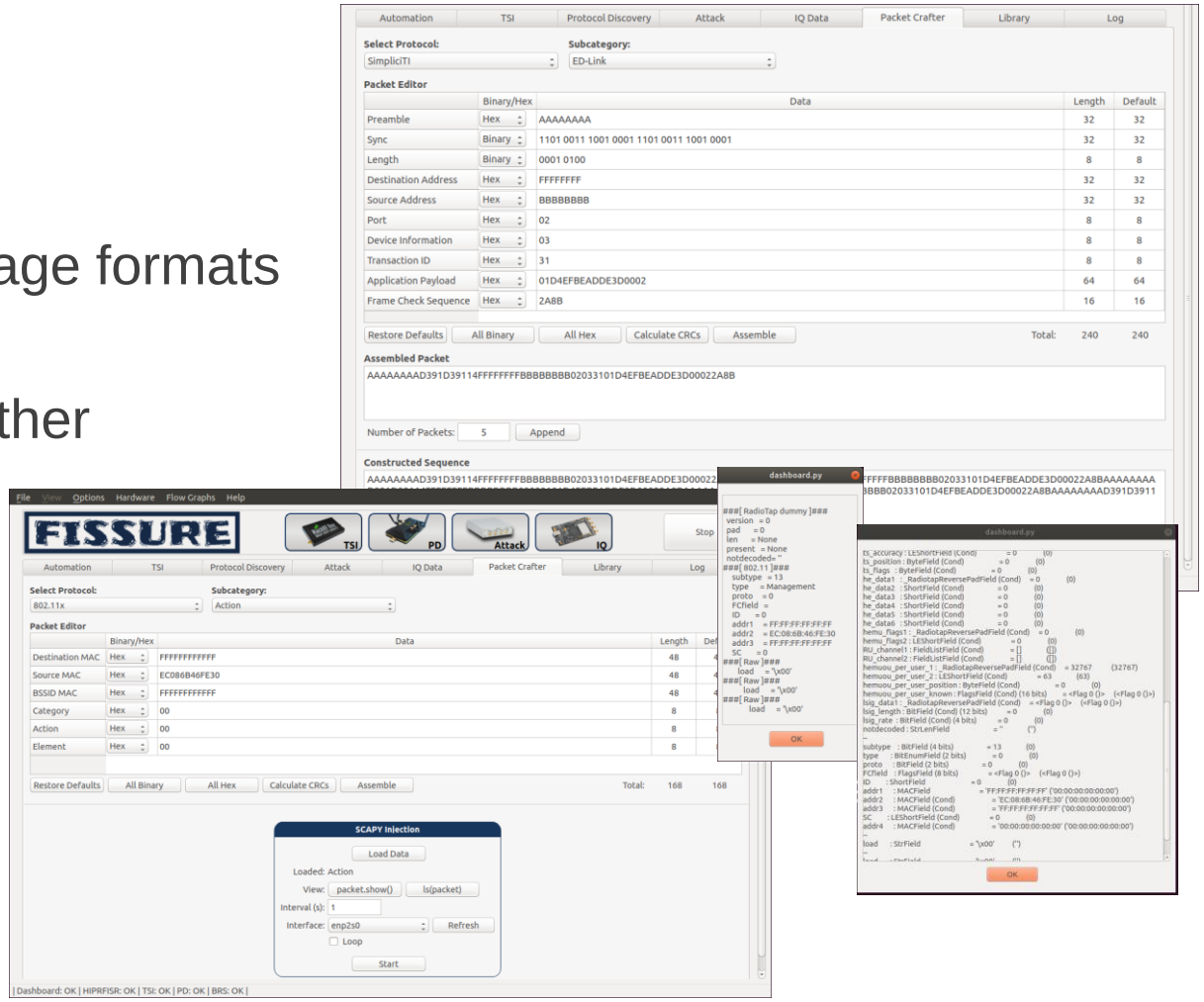
- Record
- Playback
- View
- Crop
- Append
- Overlap
- Resample
- Analyze



Current Features

Packet Crafting

- Recall common message formats and default values
- String messages together
- Scapy integration
- CRC calculation



Current Features

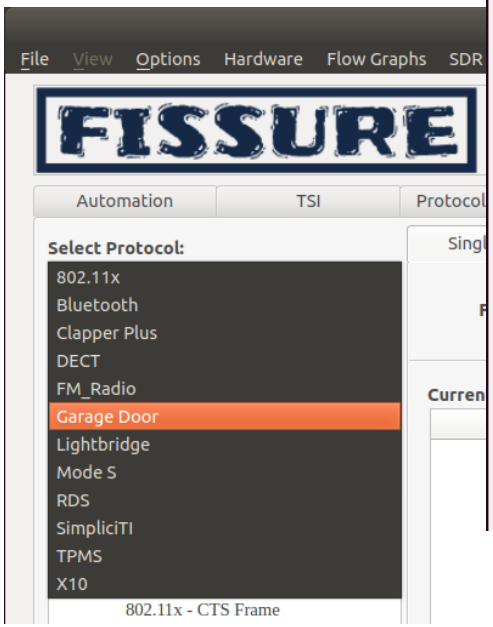
Fuzzing

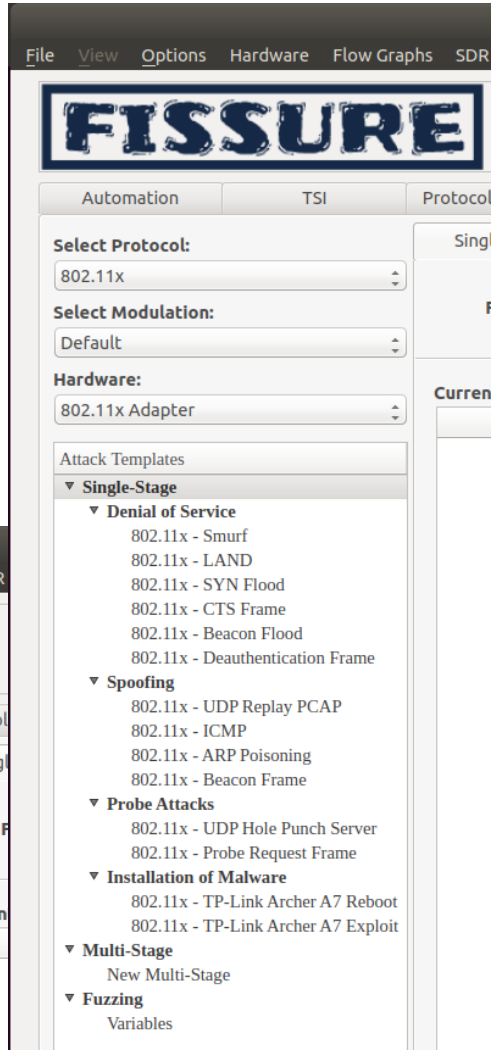
- Specify Limits, Intervals, and Seeds
- Choose What to Fuzz
  - Flow Graph Variables
  - Data Fields
- Bit-Level Fuzzing
- Automatic CRC Calculation

Current Features

Integrated Tools

- Previously developed attack vectors
- Known protocol support
- Reference flowgraphs





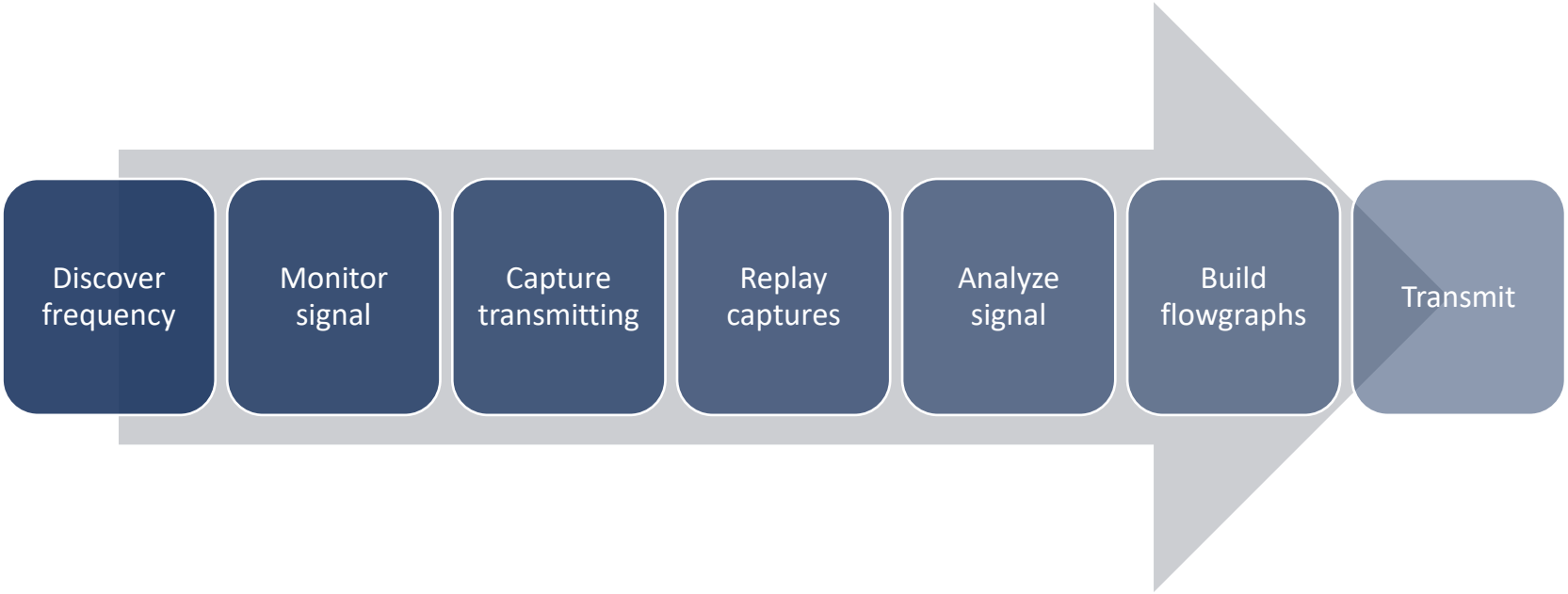
Moving Forward

- Open source
  - Encourage community collaboration
  - Expand capabilities
- Task automation
  - Machine learning based classification
  - Recursive demodulation
- Improved support
  - Add more hardware
  - Increase the integrated tools
  - More supported OS’s

Demonstration

X10 Home Automation

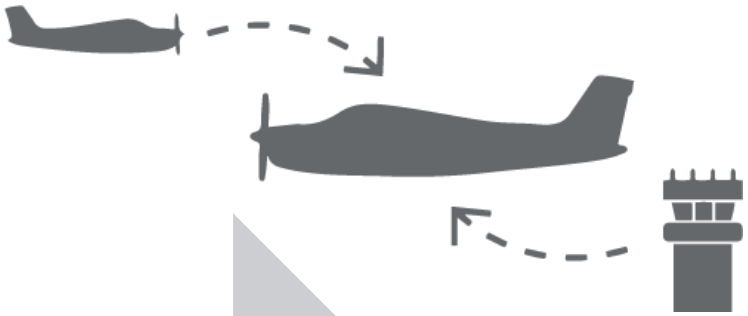
- Wireless protocol to enable “Smart” home

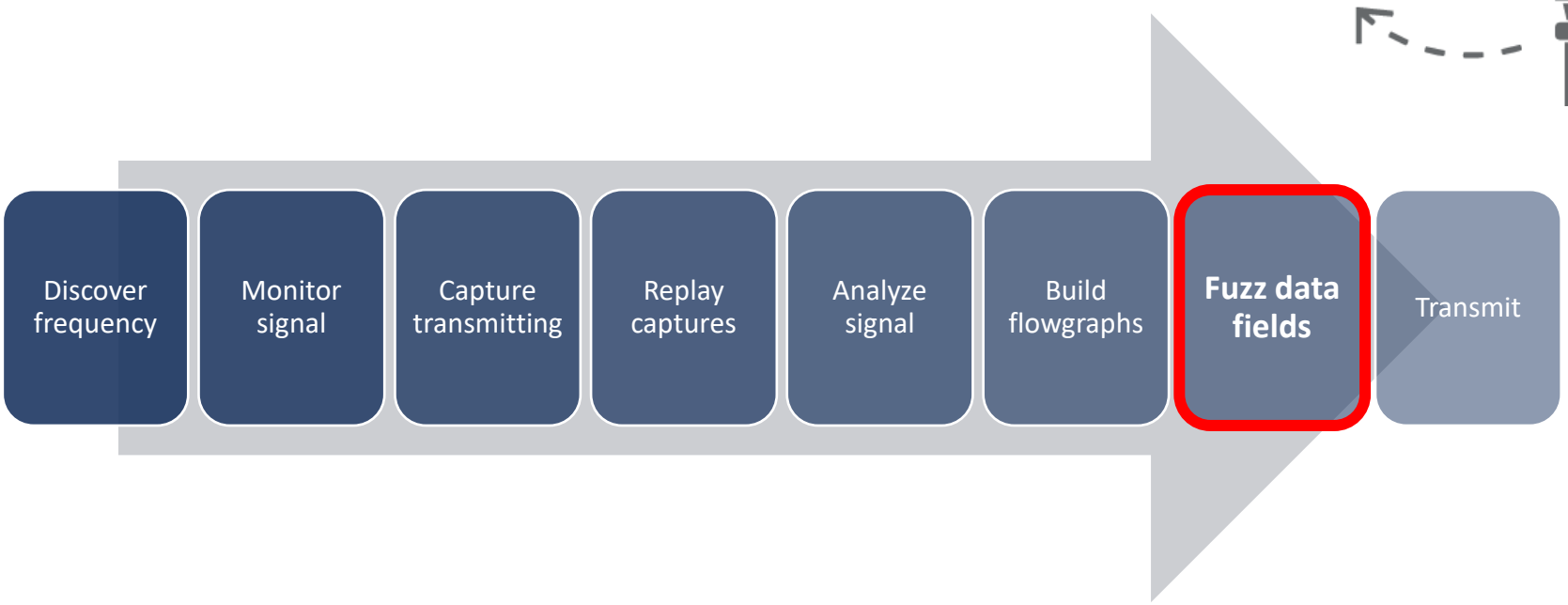


Demonstration

Automatic Dependent Surveillance–Broadcast (ADS-B)

- Aircraft location tracking and reporting





FISSURE

April 28, 2021

Any Questions

Chris Poore

Visionary

poorec@ainfosec.com

ais

WWW.AINFOSEC.COM