Automation of Electronic Attack Generation Using AI

Hal Aldridge, Ph.D.

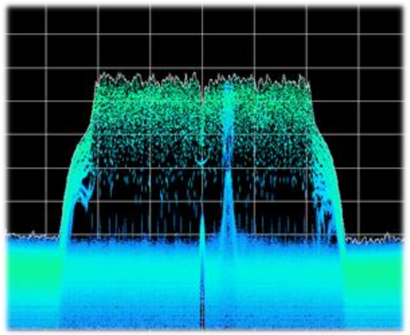
CEO, Secmation

hal.aldridge@secmation.com

Motivation – Acceleration of Technique Development

- Timelines for development of EW techniques need to be shortened to keep up with rapid changes in operational environments (ex. Ukraine)
- Advanced systems may require more agile/faster updates in techniques to be maintain effectiveness
- Many of the advanced capabilities are based on Software Defined Radios(SDR), or more generally Software Defined Receivers
- Additions of advanced spectrum agility, anti-jamming, cognitive/AI, and other capabilities are rapidly increasing the amount of software/firmware in these systems.
- ***Can AI-based methods accelerate technique development targeting these systems?***

Traditional Threats to Military Receivers



Traditional Threats

Cyber

- Attacker goal is to disrupt operation or exploit system software
- Tested by Red Teams looking mostly for common software vulnerabilities
- Layered defenses are used to protect systems

Electronic Warfare

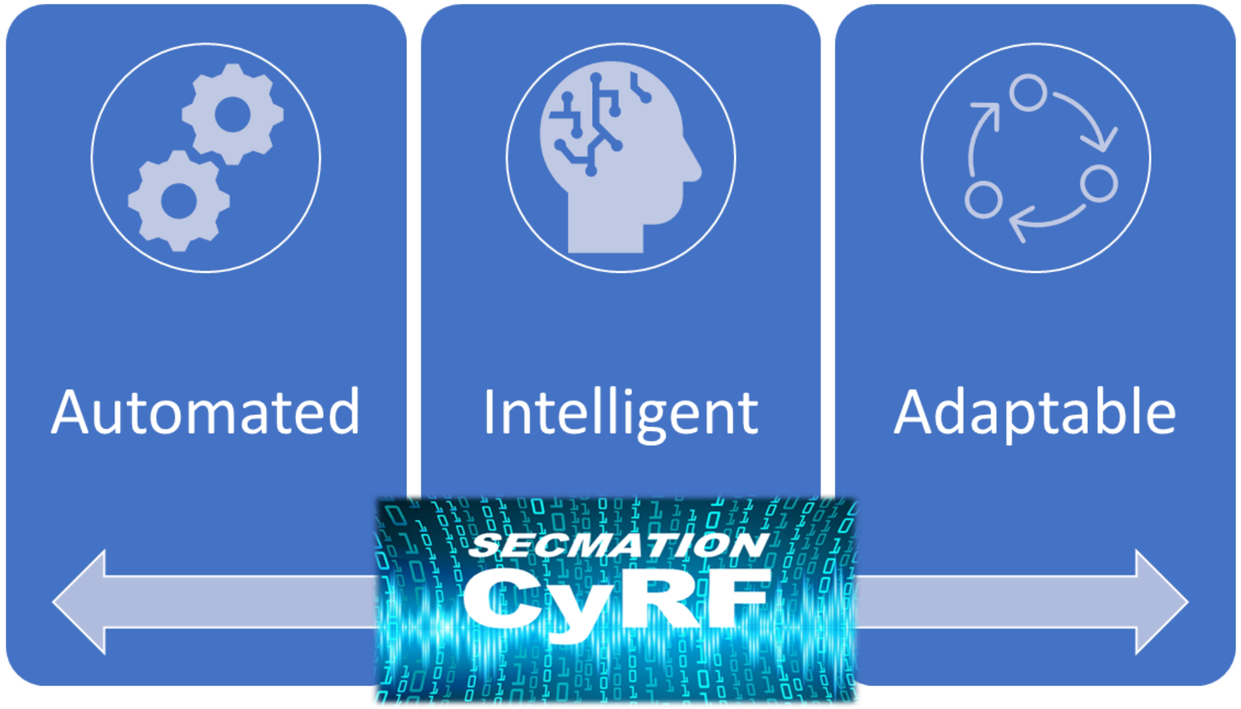
- Attacker goal is deny communications using jamming or similar method
- Systems are tested using RF signals to establish their Bit Error Rate (BER) as a measure of jamming resistance
- Protected communications use complex signals making their transmissions more difficult to jam

Emerging Integrated Threats Will Use EW Methods to Cause Cyber Effects In Software Defined Receivers

So, why aren’t integrated Cyber/EW attacks more prevalent?

- Many successful Cyber/EW attacks are “edge cases”. Like edge cases in other applications (ex. safety) they require specific combinations of parameters to happen before they will occur.
- An example effect of an edge case is an SDR software vulnerability that when exploited can significantly affect receiver operation.
- Cyber/EW edge cases in receivers are hard to find. Why?
  - Requires integrated analysis and understanding of both cyber and RF
  - Search space is large
  - Methods to effectively search for edge cases are not mature

Overcoming The Challenge – Secmation's CyRF

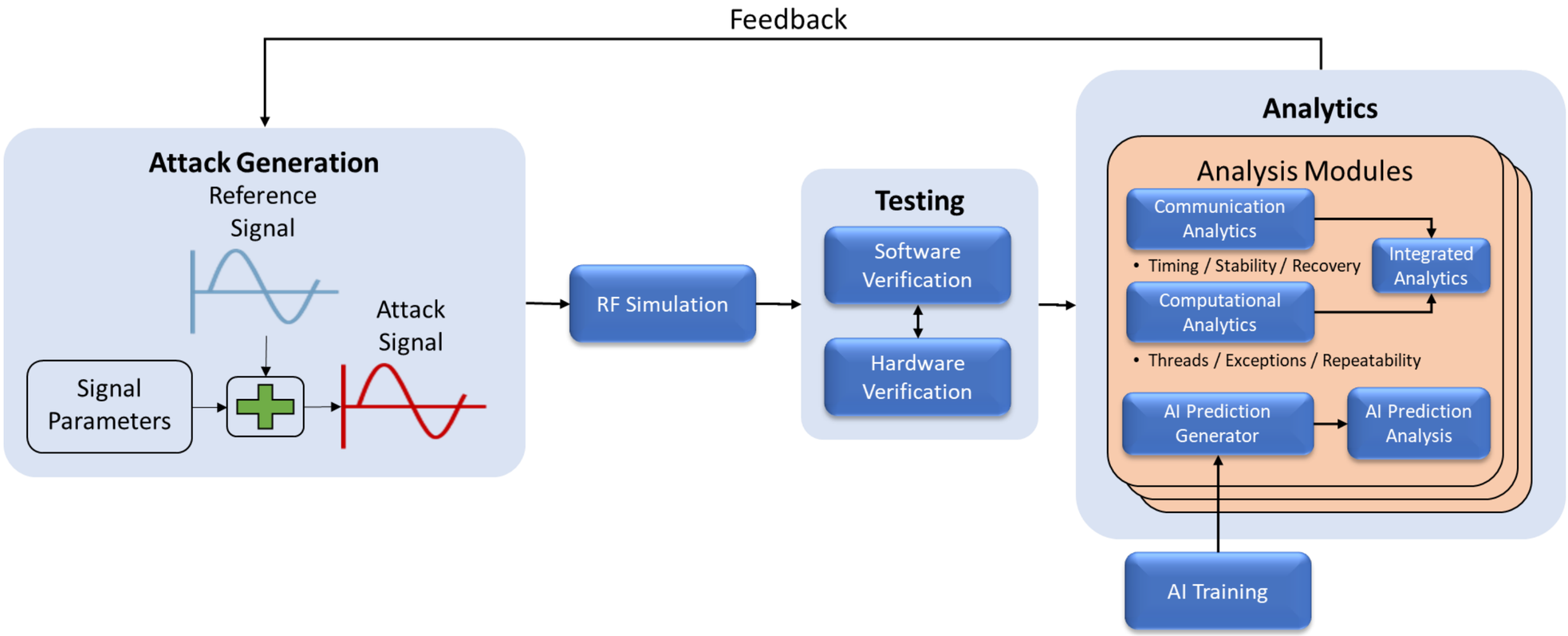


CyRF is a framework for efficiently identifying signals which exploit vulnerabilities in the signal processing software of target SDR systems

AI Driven RF-Fuzzing for Vulnerability Identification

- In cybersecurity “fuzzing” describes a specific process for searching for data that when processed by a function will cause an unintended effect (ex. divide by zero).
- The CyRF process is different. It is a true RF fuzzer creates RF signals not (think IQ data). This focus on the signals enables exploration of the software/firmware signal processing chain in the receiver.
- For vulnerability identification, our target is physical layer/waveform software that is processing the signal into data resulting in a receiver malfunction.

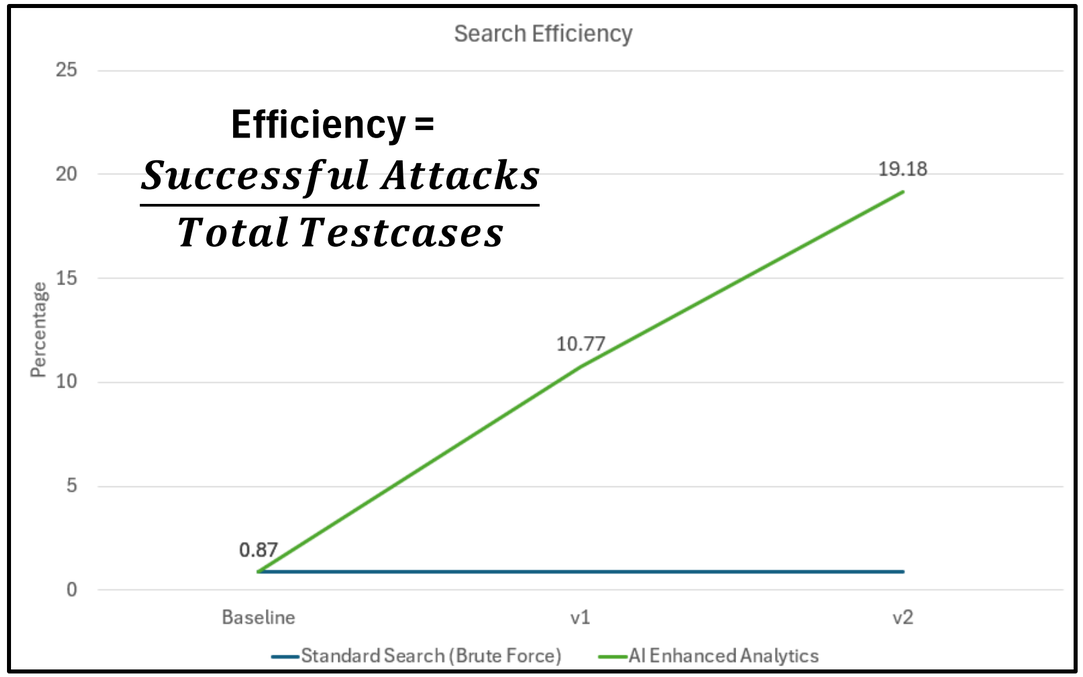
CyRF AI Guided Search Process



Use of AI significantly increases search efficiency reducing time identify working attacks.

Value of AI In Search Process

- Brute force search of an n-dimensional space is not practical and a limiting factor in using the RF fuzzing approach
- Initial application of heuristic analytics began the transition to a practical tool
- AI is showing the capability of the process to address complex real-world applications
- Initial training cycles have continued to show steady progress in search efficiency
- This translates to:
  - Finding more vulnerabilities faster
  - Better uncertainty handling



This work shows the capability of AI to find complex issues in RF design in the presence of uncertainty

Simulation vs. Data Set

- A lesson learned in development was related to effectiveness of model training.
- Initially a traditional approach was taken providing the AI model with a set of training data generated though a random search of the model.
- This method worked but the increase in performance of search using an AI trained this way did not exhibit the hoped for efficiency. This could be for several factors:
  - The data set was not large enough to provide adequate information
  - The data set did not provide the “interesting” cases needed for effective training
- These are not uncommon AI training issues
- **Using the initially trained model based on the data set to produce new data through its exploration of the simulation and retraining DID provide significant efficiency improvements.**

Synthetic Data

- An alternate use of the CyRF tool is the generation of synthetic data for use in Digital Engineering
- As an intelligent RF Fuzzer, CyRF generates signals designed to excite effects in the receiver
- The goal of the AI is determined by the metrics used to train it. In the use case discussed the metrics were related to failure mode.
- The metrics can be changed to optimize for performance parameters, different operating conditions, etc. to generate the desired effects.
- The synthetic data generation can be set to be random (ex. brute force search) to provide a baseline to compare against.

Summary

- AI can play a role in accelerating technique development targeting complex, modern RF systems
- One method to use AI is through RF fuzzing creating signals that produce the desired effects in target systems
- In addition to finding effects, systems designed for fuzzing can be used to create synthetic data sets with properties needed to support other analysis (ex. Digital Engineering)
- A key observation is that there are alternatives to the use of large datasets for training that can produce more effective AI models quicker