SCISRS
SECURING COMPARTMENTED INFORMATION WITH SMART RADIO SYSTEMS

INTELLIGENCE VALUE
The SCISRS program seeks to develop smart radio techniques to automatically detect and characterize RF anomalies that may indicate a compromise of secure data in complex RF environments. The specific types of anomalies include low probability of intercept (LPI) signals, altered or mimicked signals, and abnormal unintended emissions.

The goal of the SCISRS program is to develop smart radio techniques to automatically detect and characterize these suspicious signals and other RF anomalies in complex RF environments. The techniques must be scalable, computationally efficient, and adaptable to a range of radio hardware. IARPA's partners have established RF testbeds to evaluate algorithms at the end of each program phase. These testbeds will be replete with ordinary overt signals to form two kinds of complex RF backgrounds the Intelligence Community may operate in. Into these backgrounds, the test partners will inject various RF anomalies. In phase I, the theme will be LPI signals which are designed to be hard to detect and characterize. In phase II, the theme will be otherwise ordinary signals that have been altered in some way to carry additional information or signals that have been designed to mimic ordinary overt signals. In phase III, the theme will be anomalous emanations which are typically emitted by electronic devices (e.g., monitors, keyboards) unintentionally, thereby transmitting potentially secure information by mistake.

Examples of environments where RF anomalies may indicate compromise of secure data. In the case of the port, arriving ships may not have a current historical record of the expected RF signals. In a test range, potentially sensitive data may get transmitted into the environment. Permanent or temporary SCIFs are obvious places where data security is paramount.

PRIME PERFORMERS
- AiRANACULUS
- BAE Systems
- Expedition Technology, Inc.
- JASR Systems
- Northrop Grumman

TESTING AND EVALUATION PARTNERS
- Pacific Northwest National Laboratory

KEYWORDS
- Information security
- Signals analysis
- Machine learning
- Radio frequency communications
- Data security

PROGRAM MANAGER
Paul Kolb, Ph.D.
Phone: (301) 243-2082
Paul.kolb@iarpa.gov

www.iarpa.gov
@IARPAnews

Latest Revision: 12/14/2021