# BroBounds:

**Michael A. King**
making@sandia.gov

Sandia National Laboratories

## Technology

BroBounds is a system for auto-generating Industrial Control System (ICS) network intrusion detection (NID) rules. It takes traffic from an ICS network and provides rules that alert on violations of set-point (desired output) or sensor (observed output) boundaries. Additionally, it provides a graphical user interface to manipulate the boundaries before publishing the rules.

## Benefits

Packet analysis rules that perform application protocol deep-packet inspection are difficult to write and must be customized for each ICS asset-owner's facility. This makes it labor-intensive for the analyst and, potentially, very time consuming to produce a comprehensive ruleset for detecting anomalous behavior in control networks. BroBounds helps to solve this problem.

BroBounds provides a user interface that takes in static multi-dimensional boundary conditions for field device register values and generates a Bro configuration file that causes Bro to raise alerts when register threshold violations occur.

BroBounds generates Bro scripts that perform deep packet inspection on control system traffic. These scripts verify that boundary conditions specified by the BroBounds user for register values have not been violated

## Limits

Currently, BroBounds only works for the Modbus protocol. There are Modbus specific data structures encoded in the tool.

BroBounds only writes simple, boundary-based detection rules after processing network data values during a data capture. Therefore, more complicated analytics are currently outside the purview of BroBounds.

## Risks

BroBounds can be used entirely off-line, with packet captures from the network being captured in whatever way that the asset owner deems safe. BroBounds itself does not have any built in features that send data out over the network and thus has a very low system impact risk associated with its use.

## Deployment

Regardless of how BroBounds is deployed, the interface to the network is the packet capture/inspector program, Bro or Wireshark. This program is the primary way that data is gathered from the control network and provided to BroBounds.

With the aid of the control network engineers, an appropriate location to connect to the control network must be determined. A computer running the data capture tool (Bro, Wireshark, etc.) will be connected at the decided upon switch port (probably a SPAN port) and the program will begin data collection.

The data capture can be transferred to a computer running BroBounds for post-processing once the capture is complete.



U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2016-9903 M