U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

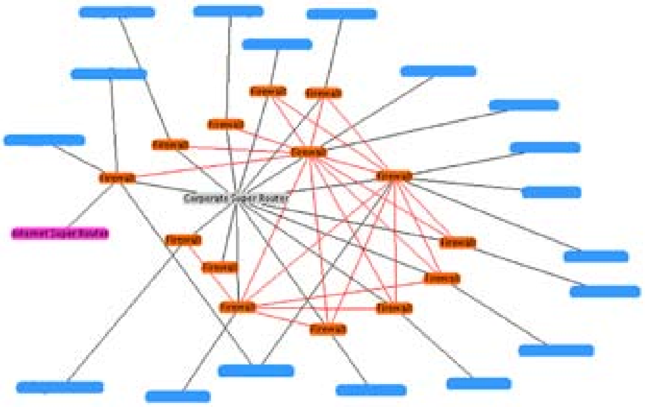
Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM)

Uses existing information to passively map control systems networks and identify cyber security perimeters

Control systems operators require a map of their energy control system network in order to identify its electronic security perimeter, critical to meeting the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards. However, purchasing active, online scanning tools specifically for network mapping can be costly, and these tools can disrupt control system function, causing system latency and possibly affecting power supply.

The ANTFARM software tool enables system operators to remotely and passively query multiple sources of existing network information, minimizing the risk of network disruption. The tool compiles output from other network analysis tools (e.g., traceroute, Nmap—which may or may not be passive), network device configuration files, firewall configuration files, and traffic logs, and correlates that data into a database.

The ANTFARM tool can utilize the data to create a visual representation of network components and connections, aiding system owners and operators in assessing their network security posture.



Sandia National Laboratories has developed the source code and detailed documentation information to allow accurate insertion and correlation of data in the ANTFARM database.

Sandia has made the source code and documentation available to all interested parties via an open-source repository website under a no-fee, general-purpose license agreement. This availability makes the tool easily accessible to control systems network security personnel, as well as other programmers, who are invited to use it for additional software projects. Access the software at http://antfarm.rubyforge.org.

National SCADA Test Bed

Benefits

- Offers control system operators a passive and remote tool to map their control system network
- Compiles and correlates large amounts of network data with minimal risk of system latency or disruption
- Assists compliance with NERC CIP standards
- Provides an open-source, no-cost software tool to identify a network's electronic security perimeter

Partners

- Sandia National Laboratories

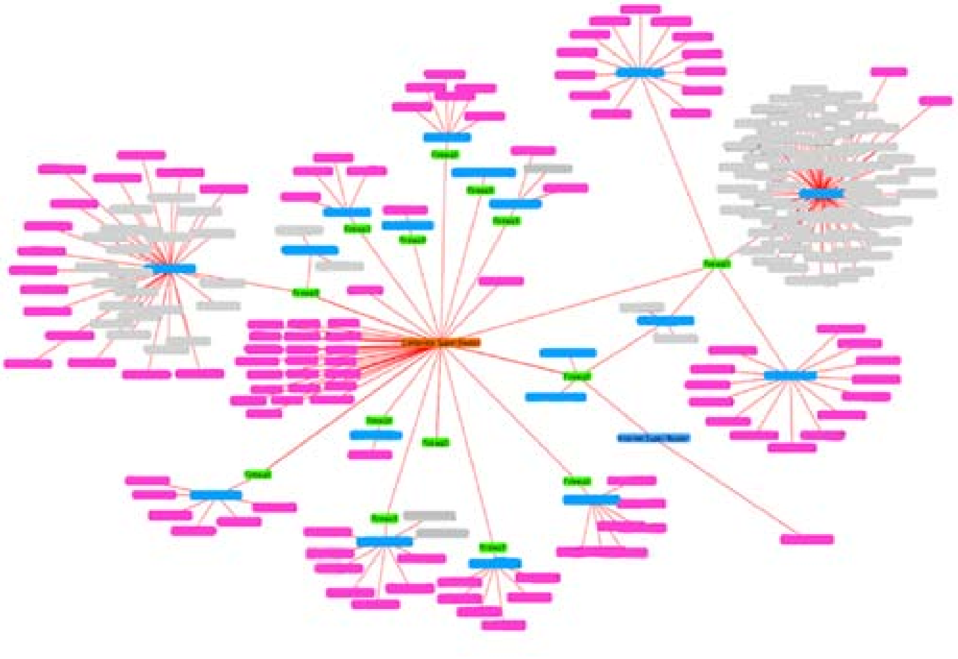
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Technical Objectives

Sandia National Laboratories' internally developed ANTFARM tool has been improved through the following project tasks:

Phase 1: Data Storage and Retrieval Algorithm

- Restructured ANTFARM source code to utilize the ActiveRecord library for the Ruby programming language, allowing easy insertion of data into the ANTFARM database
- Refined existing data parsing scripts to utilize ActiveRecord



A sample control systems network mapped by the ANTFARM tool.

Phase 2: ANTFARM Publication Material

- Described input/output requirements
- Defined the features and limitations of the tool
- Created a preliminary operator's manual
- Described a wish list of follow-on features and capabilities
- Documented code to ease future development of the tool

Phase 3: ANTFARM Training Course Materials

- Developed materials for a training course designed to educate users on how to use ANTFARM as a supplement to a broader NERC CIP vulnerability assessment
- Used the training materials developed to generate a how-to/user's guide, made available on the ANTFARM website

End Results

Projects results include:

- Source code for the software tool
- Detailed documentation for the software
- Training materials focused on how to use ANTFARM as part of a NERC CIP vulnerability assessment

This information is publicly available as open-source software under a no-fee, general purpose license agreement at http://antfarm.rubyforge.org.

By making the tool readily available, SNL invites programmers to use the code in other software projects. This will increase the utility of the information and encourage secure, concise, and rapid development of other software.

It will also make the tool immediately available for control system owners/operators to passively map their networks and increase awareness of their security posture.

August 2008

DOE National SCADA Test Bed (NSTB)

NSTB is a multi-laboratory resource that partners with industry and other government programs to test, research, and help design cyber security solutions to enhance control systems security in the energy sector and reduce the risk of energy disruption due to cyber attack.

For More Information:

Hank Kenchington
Program Manager
DOE NSTB
202-586-1878
henry.kenchington@hq.doe.gov

Bryan Richardson
Systems Engineer
Sandia National Laboratories
505-845-2386
btricha@sandia.gov

Visit Our Website:

www.oe.energy.gov/controlsecurity.htm