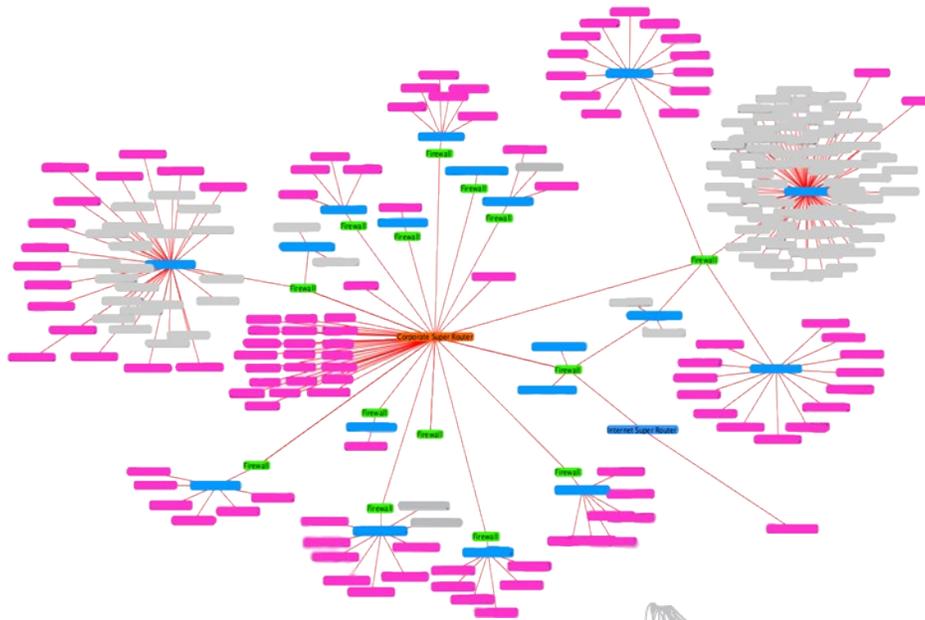


Advanced Network Toolkit for Assessments and Remote Mapping



Control System Assessment Tool

The Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM) application is a passive tool capable of safely mapping Internet Protocol (IP) networks used in industrial control systems. Such activities are required for identifying and documenting the critical cyber assets and access control modules that make up an electronic security perimeter. Traditional information technology (IT) network mapping tools can disrupt control system operations by causing system latency, inadvertently knocking scanned devices offline, etc.

Network Mapping

ANTFARM 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 existing network analysis tools (e.g., traceroute, nmap, and Nessus — which may or may not be passive), network device configuration files, firewall configuration files, and traffic logs, and correlates that data into a centralized database. The resulting aggregated data can then be visualized using a myriad of different approaches in order to aid system owners and operators in assessing their network security posture.

Benefits

ANTFARM provides IT and control system network administrators the ability to use data readily available and tools they're already familiar with to safely and effectively document and understand their control system networks. It also provides an extensible framework that allows output from new network analysis tools and configuration data formats from new network devices to be incorporated into the application.

Availability

ANTFARM is freely available under an open source license as a source code archive and as a Ruby gem. The source code can be found at github.com/ccss-sandia/antfarm and the Ruby gem can be found at rubygems.org/gems/antfarm.

For more information, contact:

Sandia National Laboratories

Bryan T. Richardson

P.O. Box 5800 MS 0671

Albuquerque, NM 87185-0671

Phone: (505) 845-2386

Email: btricha@sandia.gov



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.

UNCLASSIFIED UNLIMITED RELEASE - SAND2012-0189P