TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Automatic Verification of Network Access Control Policy Implementations

tcipg.org

Overview and Problem Statement

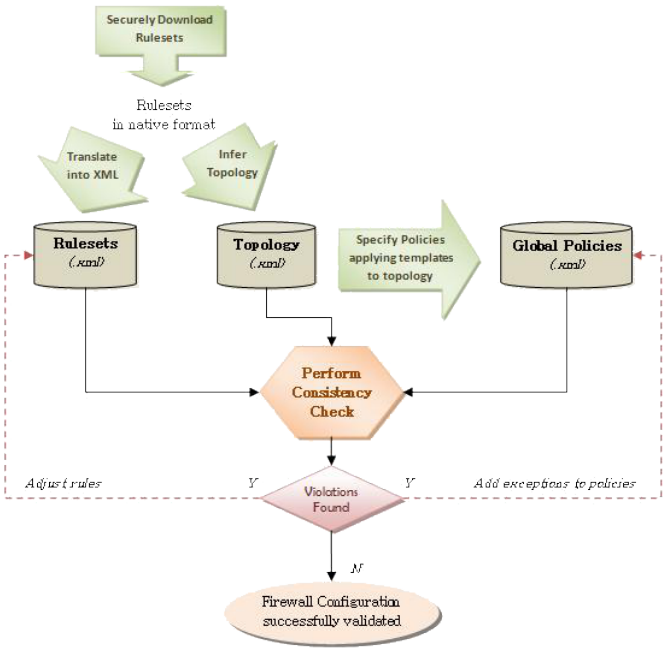
This project aims to develop a highly usable, scalable, and effective tool for analyzing security policy implementation for conformance with global security policy specification for industrial control networks. The tool provides comprehensive analysis of compliance to ensure that all access control mechanisms work collectively in harmony. The tool, called *NetAPT (Network Access Policy Tool)*, has been fully implemented and has been used successfully to aid in vulnerability assessments and compliance audits at our industry partners. NetAPT is available to potential users and has entered a final beta testing phase.

Research Objectives

- Process control networks are connected to other networks in enterprise systems; access is controlled through a large number of devices, such as firewalls.
- Best practices recommendations and compliance requirements are difficult to meet rigorously without significant man-hour investment. Pressing questions include:
    - How can we express English-language recommendations for global policy in a machine-checkable form that network administrators can easily formulate and understand?
    - How can we determine whether the access control that firewalls provide precisely meets the requirements of the machine-checkable global policy?
- Any analysis method or tool must
    - Incorporate policy rules from myriad sources.
    - Ensure scalability with size and complexity of networks.
    - Provide analytic and/or empirical demonstrations of efficacy.
- **Smart Grid Application Area:** NetAPT can be used to make sure that the access controls for the communications infrastructure of the Smart Grid are configured correctly. It can help prove compliance of the existing mechanisms with the various recommendations and standards (e.g., NERC CIP 005) and can help ensure that compliance is maintained despite any new changes to configuration of layer 3 devices (firewalls, routers).

Technical Description and Solution Approach

- NetAPT takes as input firewall configurations, and discovers the topology.
- It uses advanced data structures and modular design to incorporate a variety of policy rules and maintain extensibility.
- It has a sophisticated graphical front-end for increased usability, along with an analysis engine optimized for performance.
- The GUI and analysis engine can be decoupled and run on separate machines (GUI on an admin workstation, the engine on a powerful server). SSL is used to communicate between the two components.
- Specific optimizations for process control networks are included.
- NetAPT includes parameterized global policy templates, encoding various best practices recommendations and compliance standards that can be quickly customized to the network being analyzed.



Results and Benefits

- NetAPT has been implemented and released to select industry partners for evaluation.
- NetAPT was used for an internal audit and vulnerability assessment at a major utility, for a network with nearly 100 firewalls and several thousand hosts.
  - Helped produce comprehensive, highly visual reports to prove compliance with NERC CIP standards.
  - Identified exceptions in firewall configurations that required policy review or changes.
- NetAPT can greatly reduce the burden of managing complex security setups in large networks, allowing for creation and administration of more secure networks.
- **Partnerships and External Interactions:** Close interaction with utility partners and NERC CIP auditors.
- **Technology Readiness Level:** Development and support for NetAPT have transitioned (through a contract with DHS S&T) to commercial licensing and support; see Nicol or Sanders for details.

Researchers

- David M. Nicol, dmnicol@illinois.edu
- William H. Sanders, whs@illinois.edu
- Mouna Bamba, mbamba@illinois.edu
- Sankalp Singh, sankalp@illinois.edu
- Edmond J. Rogers, ejrogers@illinois.edu

Industry Collaborators

- Steve Coppenbarger, Cornbelt Energy
- Chris Johnson, Eastern Illini Electric Cooperative
- Kevin Perry, Southwest Power Pool (SPP)

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security