TCIPG

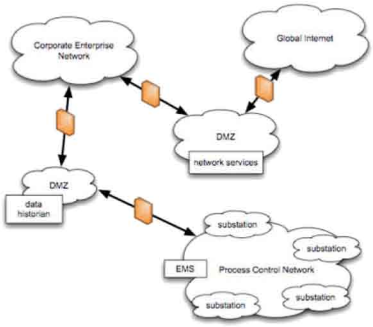
Automatic Verification of Network Access Control Policy Implementations

Sankalp Singh, David M. Nicol, William H. Sanders, Mouna Bamba, and Edmond J. Rogers

Goals

- Develop a highly usable, scalable, and effective tool for analyzing security policy implementation for conformance with global security policy specification for industrial control networks.
- Provide comprehensive analysis of compliance to make sure all access control mechanisms work collectively in harmony.

Fundamental Questions/Challenges



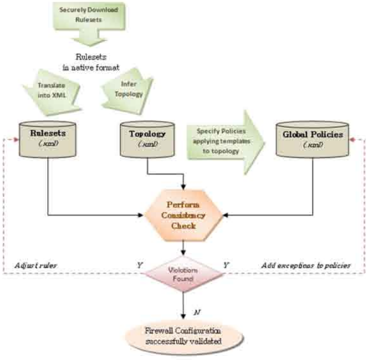
- Incorporate policy rules from a variety of sources.
- Automate and minimize user guidance.
- Ensure scalability with the size and complexity of the networks.
- Provide analytic and empirical demonstrations of efficacy.

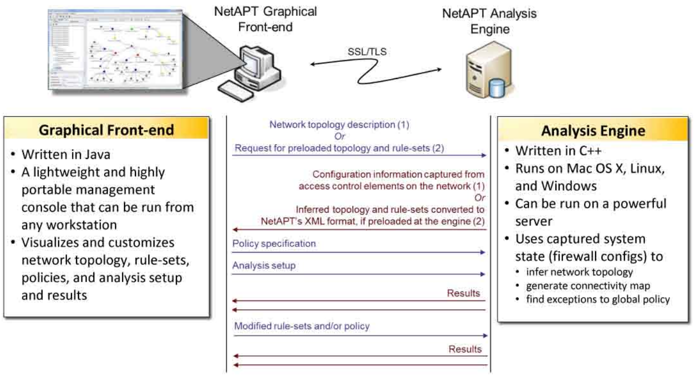
Research Plan

- Develop ability to gather rules securely from routers, firewalls (e.g., Cisco PIX, Checkpoint, SonicWall), and hosts (Windows, Linux) in control network and supporting enterprise.
- Develop algorithms for inferring the network topology from analysis of the configuration of various layer 3 devices.
- Develop algorithms and supporting data structures for analyzing all accesses for compliance with global system security specification.
- Use a multi-layered rule-graph data structure for representing network interconnectivity and data flow among enforcement rules.
- Develop a sophisticated, but easy to use, graphical front-end for the tool.
- Develop analytic proofs for time and space complexity of the various algorithms (analysis and topology inference), and completeness of topology inference algorithms.
- Automatically generate random representative process control networks (and supporting enterprise networks) based on salient characteristics of observed real industrial control networks, and use them to study tool performance.

Research Results

- NetAPT has been implemented and released to select industry partners for evaluation.


Securely Download Rulesets
Rulesets in native format
Translate into XML
Infer Topology
Rulesets (xml)
Topology (xml)
Specify Policies applying templates to topology
Global Policies (xml)
Perform Consistency Check
Adjust rules
Y
Violations Found
Y
Add exceptions to policies
N
Firewall Configuration successfully validated


NetAPT Graphical Front-end
NetAPT Analysis Engine
SSL/TLS
Network topology description (1)
Or
Request for preloaded topology and rule-sets (2)
Configuration information captured from access control elements on the network (1)
Or
Inferred topology and rule-sets converted to NetAPT's XML format, if preloaded at the engine (2)
Policy specification
Analysis setup
Results
Modified rule-sets and/or policy
Results

Graphical Front-end

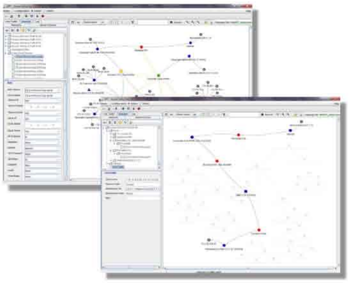
- Written in Java
- A lightweight and highly portable management console that can be run from any workstation
- Visualizes and customizes network topology, rule-sets, policies, and analysis setup and results

Analysis Engine

- Written in C++
- Runs on Mac OS X, Linux, and Windows
- Can be run on a powerful server
- Uses captured system state (firewall configs) to
  - infer network topology
  - generate connectivity map
  - find exceptions to global policy

NetAPT used for internal audit at major utility:

- Analyzed network with almost 100 firewalls and thousands of 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.



Broader Impact

- In addition to industrial control networks, the techniques developed can be used for corporate, campus, and other enterprise networks.

Future Efforts

- Further develop online assessment, statistical analysis, and extension to other access policy enforcement points.

Trustworthy Cyber Infrastructure for the Power Grid • www.tcipg.org
University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University