Assessment and Forensics for Large-Scale Smart Grid Networks

Jonathan Chu, Mirko Montanari, Xueman Mou, and Roy Campbell

Goals

We aim to improve the security and efficiency of automated systems for monitoring compliance of power systems to policies.

We introduce and analyze a secure architecture for monitoring compliance based on security event monitoring at the network level, software level, and hardware level.

Our approach is based on removing central points for monitoring to increase scalability and security.

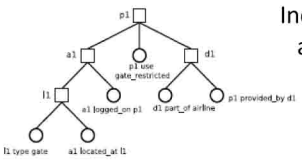
Fundamental Questions/Challenges

The centralized process used for validating compliance of power systems to policies, such as NERC CIP, cannot scale in a secure way to the systems that form the "Smart Grid."

An attacker could disrupt electricity networks by obtaining information about vulnerabilities in the system and by injecting false information into the operator.

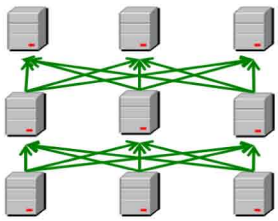
Research Plan

1) Gather policies and set up the network to distribute them across the nodes.
2) Set up redundant paths to create a more secure and robust communication framework.
3) Evaluate policy as input data come into the system.
4) Monitor the system for any anomalous policy events caused by compromised nodes.



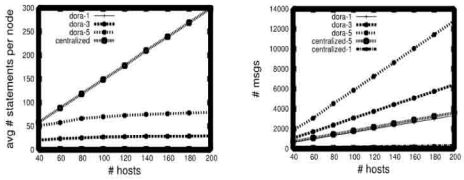
Independent, redundant aggregation trees are created to increase reliability of communication.

The compromise of one server does not affect reliability.

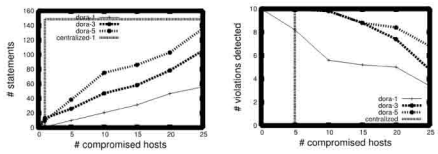


Research Results

Load for monitoring large infrastructure can be shared across a large number of non-dedicated hosts.



This hinders intruders attempting to attack the system.



Confidentiality impact: number of statements about the system obtained by an attacker that compromises x number of hosts

Integrity impact: number of violations detected when x hosts are compromised

Broader Impact

This distributed, secure architecture could be applied to power systems that use distributed computing to transport data like power meter readings, sensor measurements, logs of activity, pressure, and more.

Interaction with Other Projects

The research that built up to this project was done with the collaboration of Boeing and the Assured Cloud Computing Center at the University of Illinois.

Future Efforts

- An implementation and measurements of this distributed architecture within the TCIPG testbed
- Further analysis of performance in more realistic environments
- Enhancements and modifications to the architecture to increase efficiency and load balancing